

# EWENS SAMPLING AND INVARIABLE GENERATION

GERANDY BRITO, CHRISTOPHER FOWLER, MATTHEW JUNGE, AND AVI LEVY

**ABSTRACT.** We study the number of random permutations needed to invariably generate the symmetric group,  $S_n$ , when the distribution of cycle counts has the strong  $\alpha$ -logarithmic property. The canonical example is the Ewens sampling formula, for which the number of  $k$ -cycles relates to a conditioned Poisson random variable with mean  $\alpha/k$ . The special case  $\alpha = 1$  corresponds to uniformly random permutations, for which it was recently shown that exactly four are needed.

For strong  $\alpha$ -logarithmic measures, and almost every  $\alpha$ , we show that precisely  $\lceil (1 - \alpha \log 2)^{-1} \rceil$  permutations are needed to invariably generate  $S_n$ . A corollary is that for many other probability measures on  $S_n$  no bounded number of permutations will invariably generate  $S_n$  with positive probability. Along the way we generalize classic theorems of Erdős, Tehran, Pyber, Luczak and Bovey to permutations obtained from the Ewens sampling formula.

## CONTENTS

1. Introduction	1
1.1. Ewens sampling and the logarithmic property	2
1.2. Statement of Theorem 1	3
1.3. Generalizations for the Ewens sampling formula	5
1.4. Overview of proof and result for sumsets	6
1.5. Further questions	7
1.6. Notation	8
1.7. Outline of paper	9
1.8. Acknowledgements	9
2. Proof of Theorem 1	9
3. The upper bound for $m_\alpha$	11
3.1. The Feller Coupling	11
3.2. Proofs of Theorem 3, Theorem 4, and Theorem 5	17
3.3. Proving Proposition 7	24
4. The upper bound for $s_\alpha$	25
5. The lower bound for $s_\alpha$	28
References	33

## 1. INTRODUCTION

In 1934, van der Waerden raised the question of the minimal number of uniformly random permutations required to invariably generate  $S_n$  with positive probability [Wae34]. Recent breakthroughs by Pemantle, Peres, Rivin [PPR15] and Eberhard, Ford, Green [EFG15a] resolved van der Waerden's question, showing that precisely four permutations are required.

We consider the same question in the context of more general permutation measures related to the cycle structure, primarily the Ewens sampling formula (1) introduced in [Ewe72]. It aligns a permutation's cycle structure with conditioned independent Poisson random variables.

Elements  $g_1, \dots, g_m$  of a group  $G$  *generate* the group if the smallest subgroup containing them is  $G$  itself. The *symmetric group*  $S_n$  is the group of permutations of the set  $[n] := \{1, \dots, n\}$ . Permutations  $\pi_1, \dots, \pi_m$  *invariably generate*  $S_n$  if for all  $\sigma_1, \dots, \sigma_m \in S_n$  the elements  $\sigma_1 \pi_1 \sigma_1^{-1}, \dots, \sigma_m \pi_m \sigma_m^{-1}$  generate  $S_n$ . The definition of invariable generation is conjugacy invariant. Conjugacy classes of the symmetric group are parametrized by the *cycle type* of a permutation, defined to be the multiset of cycle lengths in the cycle decomposition of a permutation. For this reason, invariable generation concerns only the cycle structure of permutations, rather than the action on  $[n]$ .

Recent developments show that cycle counts converge to independent Poisson random variables for many measures on  $S_n$  as  $n$  tends to infinity. Arratia, Barbour and Tavaré have shown that strong  $\alpha$ -logarithmic measures have this property and numerous further results [AT92, ABT92, ABT00, ABT16]. Measures with general cycle weights are considered in [BUV11, EU14] and related permutons are introduced in [KKRW15]. Following this work, Mukherjee used Stein's method to deduce that a variety of permutation measures have Poisson limiting cycle counts [Muk16]. Furthermore, the structure of the short cycles in the Mallows measure was characterized in [GP16].

In addition to its intrinsic interest, the minimal number of permutations required for invariable generation has applications to computational Galois theory. One may use this quantity to estimate the runtime of a Monte Carlo polynomial factorization algorithm [Mus78, Hei86, DS00, PPR15]. This establishes a connection between the irreducible factors of polynomials and the cycle structure of permutations. The cycle structure of a permutation is also compared with prime factorization of integers in the survey [Gra08]. An analogy between divisors of large integers and invariable generation of permutations is then mentioned in the introduction of [EFG15a], postulating a link between the threshold for invariable generation and small divisors of a set of random integers.

Despite the age of van der Waerden's question, it was only recently shown that the number of uniformly random permutations required to invariably generate  $S_n$  is bounded. A bound of  $O(\sqrt{\log n})$  was first established in [Dix92]. This was improved to  $O(1)$  in [LP93], but the constant was large ( $\approx 2^{100}$ ). Pemantle, Peres and Rivin reduced the bound to four in [PPR15], which was then shown to be sharp by Eberhard, Ford and Green in [EFG15a].

We extend the results for uniform permutations to the Ewens' sampling formula and beyond. Along the way, we extend results in [ET67, LP93, Bov80], replacing counting arguments with a tool known as the Feller coupling (8) introduced in [Fel45, p. 815].

**1.1. Ewens sampling and the logarithmic property.** The Ewens sampling formula appears throughout mathematics, statistics and the sciences. In the words of Harry Crane it, “exemplifies the harmony of mathematical theory, statistical application, and scientific discovery.” This is stated in his survey [Cra16b]. It and its followup [Cra16a] give a nice tour of the formula's universal character, describing applications to evolutionary molecular genetics, the neutral theory of biodiversity, Bayesian nonparametrics, combinatorial stochastic processes, and inductive inference, to name a few. The sampling formula also underpins foundational mathematics in number theory, stochastic processes, and algebra.

We start by formally defining the *Ewens sampling formula*, as well as the strong  $\alpha$ -logarithmic property. Let  $\text{Poi}(\lambda)$  denote the law of a Poisson random variable with mean

$\lambda$ . Fix  $\alpha > 0$  and let  $X_1, \dots, X_n$  be independent random variables in which  $X_k$  has law  $\text{Poi}(\alpha/k)$ . For a permutation  $\pi \in S_n$  let  $C_k$  denote the number of  $k$ -cycles in  $\pi$ . More precisely,  $C_k$  is the number of disjoint  $k$ -element subsets of  $[n]$  on which  $\pi$  restricts to a cyclic permutation. We say that the vector  $\mathbf{C} = (C_1, \dots, C_n)$  has distribution  $\text{ESF}(\alpha, n)$  if it satisfies the joint distribution:

$$(1) \quad \mathbf{P}[C_1 = x_1, \dots, C_n = x_n] = \mathbf{P}\left[X_1 = x_1, \dots, X_n = x_n \mid \sum_{k=1}^n kX_k = n\right].$$

The tuple  $(C_1, \dots, C_n)$  uniquely specifies the cycle type of a permutation. Furthermore, it is easy to see that as  $\pi$  ranges over  $S_n$ , the tuple  $(C_1, \dots, C_n)$  associated to  $\pi$  ranges over the set

$$\left\{ (C_1, \dots, C_n) \in \{0, \dots, n\}^n : \sum_{k=1}^n kC_k = n \right\}.$$

Thus, (1) specifies a measure on the conjugacy classes of  $S_n$ . We extend this to a measure on  $S_n$  (also denoted by  $\text{ESF}(\alpha, n)$ ) by weighting all elements of the same class uniformly. Note that  $\text{ESF}(1, n)$  is the uniform measure, and therefore the results we establish regarding  $\text{ESF}(\alpha, n)$  will generalize the corresponding results about uniform permutations appearing in [PPR15, EFG15a].

A more general family that includes  $\text{ESF}(\alpha, n)$  is obtained by replacing the  $X_k$  in (1) with an arbitrary sequence of independent nonnegative integer valued random variables  $Z_1, Z_2, \dots$ . To avoid intractable distortions when conditioning on  $\sum kZ_k = n$ , logarithmic growth of  $\sum Z_k$  is traditionally assumed (see [ABT00]). For our purposes, we require the  $Z_k$  satisfy the *strong  $\alpha$ -logarithmic condition*:

$$(2) \quad \begin{aligned} |i\mathbf{P}[Z_i = 1] - \alpha| &< e(i)c_1, \\ i\mathbf{P}[Z_i = \ell] &\leq e(i)c_\ell, \quad \ell \geq 2, \\ \text{where } \sum i^{-1}e(i) \text{ and } \sum \ell c_\ell &\text{ are both finite.} \end{aligned}$$

Besides Poisson, the most commonly used distributions for the  $Z_i$  are the negative-binomial and binomial distributions. These are called assemblies, multisets, and selections, respectively (see [ABT00] for more discussion). The proof that all three of these different distributional choices for the  $Z_i$  satisfy the strong  $\alpha$ -logarithmic property is in [ABT00, Proposition 1.1].

It is no trouble to work at this level of generality, because the limiting cycle structure of any family satisfying the strong  $\alpha$ -logarithmic property is the same as that for an  $\text{ESF}(\alpha, n)$  permutation. We will describe this in more detail in Section 1.4, but in short, the number of  $\ell$ -cycles converges to an independent Poisson with mean  $\alpha/\ell$ .

**1.2. Statement of Theorem 1.** We state our result in terms of random variables  $Z_1, Z_2, \dots$  satisfying the strong  $\alpha$ -logarithmic property at (2). The example to keep in mind though is the measure  $\text{ESF}(\alpha, n)$ , since all of these have the same limiting cycle counts.

Given such a collection let  $\mu_n(\alpha, Z_1, Z_2, \dots, Z_n)$  be the measure induced on  $S_n$  via the relation at (1) with  $X_k$  replaced by  $Z_k$ . We define  $m_\alpha = m_\alpha(Z_1, Z_2, \dots)$  to be the minimum number of permutations sampled according to  $\mu_n$  to invariably generate  $S_n$  with positive probability as  $n \rightarrow \infty$ :

$$(3) \quad m_\alpha = \inf_{m \geq 2} \left\{ m : \inf_{n \geq 2} \mathbf{P}[\{\pi_1, \dots, \pi_m\} \subset S_n, \pi_i \sim \mu_n, \text{ invariably generate } S_n] > 0 \right\}.$$

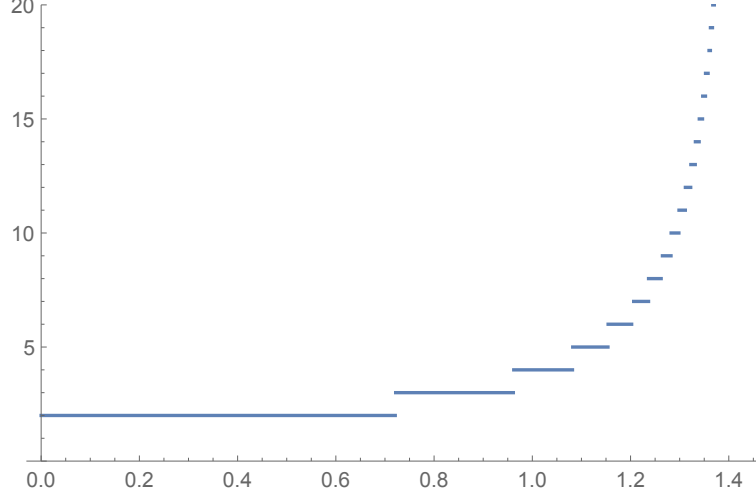


FIGURE 1. The graph  $h(\alpha)$  defined at (4), and thus the behavior of  $m_\alpha$  and  $s_\alpha$ . We are not sure about the value at the points of discontinuity in  $h$ . See Question 1 for more discussion.

Our theorem gives a closed formula for  $m_\alpha$  (see Figure 1), save for a countable exceptional set. Because we will reference it several times, we write the expression here:

$$(4) \quad h(\alpha) = \begin{cases} \lceil (1 - \alpha \log 2)^{-1} \rceil, & 0 < \alpha < 1/\log 2 \\ \infty, & \alpha \geq 1/\log 2 \end{cases}.$$

**Theorem 1.** *Let  $Z_1, Z_2, \dots$  be a collection of random variables satisfying the strong  $\alpha$ -logarithmic condition at (2). Let  $m_\alpha = m_\alpha(Z_1, Z_2, \dots)$ , as in (3), be the minimum number of permutations to invariably generate  $S_n$  with positive probability. Let  $h(\alpha)$  be as in (4). For points of continuity of  $h$  it holds that  $m_\alpha = h(\alpha)$ . At points of discontinuity we have  $h(\alpha) \leq m_\alpha \leq h(\alpha) + 1$ .*

This has broader implications beyond measures that have the strong  $\alpha$ -logarithmic property. We use it to deduce that any finite collection of random permutations with cycle counts asymptotically dominating a  $\text{Poi}(1/j \log 2)$  random variable will fail to generate a transitive subgroup of  $S_n$ .

**Corollary 2.** *Suppose that  $c_j \geq 1/\log 2$  and  $X_k \sim \text{Poi}(c_j/j)$ . Let  $\kappa_n$  be a sequence of probability measures on  $S_n$  such that for random permutations  $\pi \sim \kappa_n$  the cycle structure,  $\mathbf{C}$  satisfies*

$$d((C_1, \dots, C_{k_0}), (X_1, \dots, X_{k_0}))_{TV} \rightarrow 0$$

*for all fixed  $k_0$ . Then, the probability that any fixed number of permutations sampled according to  $\kappa_n$  invariably generate a transitive subgroup of  $S_n$  goes to 0 as  $n \rightarrow \infty$ .*

This corollary is particularly relevant to the results in [BUV11] and [EU14]. They describe measures on  $S_n$  that are formed by weighting cycle lengths by parameters  $c_j$ . The limiting cycle structure has  $C_j \sim \text{Poi}(c_j/j)$ . Thus, we can create any limiting Poisson cycle structure we like. In particular, those satisfying Corollary 2.

Another source of alternate measures with limiting Poisson cycle counts comes from [Muk16]. This fits into the larger body of work on permutons initiated in [KKRW15]. Of

particular interest is Mallow's measure (introduced in [Mal57]). This measure specifies a parameter  $q_n > 0$  that biases towards more or less inversions in a permutation. A permutation  $\pi$  has probability proportional to  $q_n^{\text{inv}(\pi)}$ , where  $\text{inv}(\pi) := |\{(s, t) | s < t \text{ and } \pi s > \pi t\}|$ .

The recent article ([GP16]) begins to characterize the cycle structure of Mallow's measure. They find that for  $(1 - q_n)^{-2} \ll n$  all cycles are on the order of  $o(n)$ . The high density of small cycles, along with [Muk16, Theorem 1.4], which proves a limiting Poisson cycle profile, suggests that no finite collection of permutations sampled according to Mallow's measure in this regime will invariable generate  $S_n$ . Note that in the regime  $(1 - q_n)^{-2} \gg n$  the cycle counts converge to those of a uniformly random permutation. This is a new and exciting area. We are hopeful our result will find more applications as these objects become better understood.

**1.3. Generalizations for the Ewens sampling formula.** In proving Theorem 1 we connect an approximation sumset model (described in Section 1.4) back to fixed-set sizes in random permutations. This also takes place in [PPR15] and [EFG15a]. These two articles use a small-cycle limit theorem for uniformly random permutations ([AT92, Theorem 1]). Namely, that the number of  $\ell$ -cycles in a uniformly random permutation converges to a Poisson random variable with mean  $1/\ell$  that is independent of the other small cycles.

Permutations sampled from  $\mu_n$  have an analogous limit theorem ([ABT00, Theorem 3.2]). Except now the  $\ell$ -cycles behave like Poisson random variables with mean  $\alpha/\ell$ . This lets us use similar ideas to analyze the corresponding sumset model. However, our approach diverges significantly when we connect back to random permutations. Especially in obtaining an upper bound on  $m_\alpha$ . The difference is that both [PPR15] and [EFG15a] have access to a large canon of results for uniformly random permutations. We do not. This requires a deep excavation where we extend classical results to  $\pi \sim \text{ESF}(\alpha, n)$ . Along the way we prove many new estimates (see Lemma 10, Lemma 11, Lemma 12, Proposition 13, Lemma 17, and Lemma 19) for larger cycle lengths in  $\text{ESF}(\alpha, n)$  permutations.

We begin by showing that with high probability the only transitive subgroups containing a permutation  $\pi$  sampled with distribution  $\text{ESF}(\alpha, n)$  are  $A_n$  and  $S_n$ . This is the analogue of what [LP93, Theorem 1] proves for uniformly random permutations. This was recently studied in more detail by Eberhard, Ford, Green in [EFG15b]. We plan to explore this vein for  $\text{ESF}(\alpha, n)$  permutations in future work. For our current purposes, the following result suffices.

**Theorem 3.** *Let  $\pi \sim \text{ESF}(\alpha, n)$ . Then with probability  $1 - o(1)$  the only transitive subgroups containing  $\pi$  are  $A_n$  and  $S_n$ .*

Pyber and Luczak rely on an important theorem of Bovey regarding primitive subgroups. We need the analogue of it for  $\text{ESF}(\alpha, n)$  permutations. The *minimal degree* of  $\langle \pi \rangle = \{\pi^k : k \in \mathbb{Z}\}$  is the minimum number of elements of  $\{1, \dots, n\}$  displaced by some power of  $\pi$ .

[Bov80, Theorem 1] says that if  $\pi$  is a uniformly random permutation, then for each  $\varepsilon > 0$  and  $0 < \beta < 1$  we have

$$\mathbf{P}[\text{minimal degree of } \langle \pi \rangle > n^\beta] < C_{\varepsilon, \beta} n^{\varepsilon - \beta}.$$

We establish a weaker analogue of this result.

**Theorem 4.** *Let  $\pi \sim \text{ESF}(\alpha, n)$ . For each  $0 < \beta < 1$  and any  $\alpha$  it holds that*

$$\mathbf{P}[\text{minimal degree of } \langle \pi \rangle > n^\beta] = o(1).$$

Establishing Theorem 3 also requires a generalization of a classical theorem of Erdős and Turán (see [ET67, Theorem V]).

**Theorem 5.** *Let  $\pi \sim \text{ESF}(\alpha, n)$  and  $\omega(n) \rightarrow \infty$ . The probability that the largest prime which divides  $\prod_{\ell=1}^n \ell^{C_\ell}$  is larger than  $n \exp(-\omega(n)\sqrt{\log n})$  is  $1 - o(1)$ .*

The proof of Theorem 3 uses both Theorem 4 and Theorem 5. For all three generalizations we follow a somewhat similar blueprint to their predecessors. However, the previous work often uses special features of uniformly random permutations. Counting arguments are heavily employed. In general, these techniques do not translate to  $\text{ESF}(\alpha, n)$  permutations. Our approach is to use the Feller coupling (see Section 3.1) to directly relate the cycle structure to independent Poisson random variables. In some places this yields more elegant proofs, in others it becomes a bit technical. Keeping in mind that  $\text{ESF}(1, n)$  is the uniform measure, this is a nice high-level approach to extending these results.

**1.4. Overview of proof and result for sumsets.** Because a fixed set's size is a sum of cycle lengths of a permutation, invariable generation is related to sumsets formed from random multisets. The link is developed over a collaborative arc of Arratia, Barbour and Tavaré, [ABT92, ABT00, AT13, ABT16]. They study the relationship between  $\alpha$ -logarithmic structures and Poisson random variables. Most relevant for our purposes are the descriptions of the cycle counts  $\mathbf{C} = (C_1, \dots, C_n)$  for permutations sampled according to  $\mu_n$ .

They prove in [ABT00, Theorem 3.1, Theorem 3.2] that, for permutations induced by the strong  $\alpha$ -logarithmic property, the small cycle counts evolve to be independent Poisson random variables, and the large cycle counts follow Ewens sampling formula. Furthermore, [ABT92, Lemma 1] (also discussed in [ABT16]) shows that the Ewens sampling formula can be cleanly related via the Feller coupling to independent  $\text{Poi}(\alpha/k)$  random variables. The payoff is that we can model the sizes of fixed sets in a permutation with independent Poisson random variables.

Let  $\mathbf{X}(\alpha) = (X_1, X_2, \dots)$  be a sequence of Poisson random variables where  $X_j$  has mean  $\alpha/j$ . The coupling discussed in the previous paragraph allows us to model the sizes of fixed sets in a permutation with the random sumset

$$\mathcal{L}(\mathbf{X}(\alpha)) = \left\{ \sum_{j \geq 1} jx_j : 0 \leq x_j \leq X_j \right\}.$$

Returning to our opening question, we can bound the required number of permutations from above if no fixed set size is common to all permutations. And we can bound the number from below if there is guaranteed to be a common fixed set size. Consider independent realizations  $\mathbf{X}^{(1)}(\alpha), \dots, \mathbf{X}^{(m)}(\alpha)$ . The upper and lower bounds correspond to finding extremal values of  $m$  such that

- (i)  $\bigcap_{i=1}^m \mathcal{L}(\mathbf{X}^{(i)}(\alpha)) = \{0\}$  with positive probability, and
- (ii)  $|\bigcap_{i=1}^m \mathcal{L}(\mathbf{X}^{(i)}(\alpha))| = \infty$  almost surely.

Since common elements among independent sumsets correspond to common fixed-set sizes of independent permutations, invariable generation is analogous to a trivial sumset intersection. On the other hand, an infinite intersection means that common fixed-sets persist among the permutations. For the case  $\alpha = 1$ , the results of [PPR15, Theorem 1.6] and [EFG15a, Corollary 2.5] each imply that four sets suffice in (i). That (ii) holds with three sets is due to [EFG15a, Corollary 3.9]. Here is the analogue for general  $\alpha > 0$ .

**Theorem 6.** *Let  $s_\alpha := \inf\{m : \mathbf{P}[\bigcap_1^m \mathcal{L}(\mathbf{X}^{(i)}(\alpha)) = \{0\}] > 0\}$  be the smallest number of i.i.d. sumset intersections so that the resulting set is trivial with positive probability. Let  $h(\alpha)$*

be as in (4), and  $m_\alpha$  as in Theorem 1. At points where  $h$  is continuous we have  $s_\alpha = h(\alpha)$ , and at the discontinuities  $h(\alpha) \leq s_\alpha \leq h(\alpha) + 1$ .

To establish this result for sumsets, we build upon the ideas in [PPR15] and [EFG15a] to prove matching lower and upper bounds for  $s_\alpha$ . These bounds can be found in Proposition 23 and Proposition 24. Parts of the argument are as simple as swapping 1's for  $\alpha$ 's, but in others, particularly the lower bound, some care is required.

A relevant quantity for establishing the upper bound is  $p_k = p_k(\alpha)$ , the probability the element  $n$  appears in  $\mathcal{L}(\mathbf{X})$ . Estimating  $p_k(1)$  is the major probabilistic hurdle in [PPR15]. There are two difficulties. The first is called a lottery effect; certain unlikely events greatly skew  $p_k$ . This is circumvented by using *quenched* probabilities  $\tilde{p}_k$ , which ignore an  $o(1)$  portion of the probability space (that  $\sum X_j$  and  $\sum jX_j$  are uncharacteristically large). With this restriction, it is shown in [PPR15, Lemma 2.3] that  $\tilde{p}_k(1) \leq k^{\log(2)-1}$ . Notice that  $4(\log 2 - 1) < -1$  and a Borel-Cantelli type argument implies finiteness of the intersection. Establishing the quenched formula is the second hurdle. It requires a clever counting and partitioning of  $\mathcal{L}(\mathbf{X})$ . We generalize these ideas in Lemma 22 to obtain the upper bound

$$\tilde{p}_k(\alpha) \leq C_\varepsilon k^{-1+\alpha \log 2 + \varepsilon}$$

for any  $\varepsilon > 0$ . Taking into account the lottery effect, and ignoring a vanishing portion of the probability space, we can write  $\mathbf{P}[k \in \cap_1^m \mathcal{L}(\mathbf{X}^{(i)})] = \prod_1^m \tilde{p}_k$ . When  $m \geq \lceil (1 - \alpha \log 2 + \varepsilon)^{-1} \rceil$ , the product is smaller than  $n^{-1}$ , and the probabilities are summable. With this, the Borel-Cantelli lemma implies the intersection is almost surely finite, and thus it is trivial with positive probability.

The lower bound in Proposition 24 requires more care. We generalize the framework in [EFG15a, Section 3] to higher dimensions to incorporate more than three sumsets as well as different values of  $\alpha$ . Given  $I \subseteq \mathbb{N}$  and  $m$  sumsets we consider the set of differences

$$S(I; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}) := \{(n_1 - n_m, n_2 - n_m, \dots, n_{m-1} - n_m) : n_i \in \mathcal{L}(\mathbf{X}^{(i)}) \cap I\}.$$

We use Fourier analysis (as in [EFG15a] and [MT84]) to study a smoothed version of the indicator function of this set. In particular, we will work with its Fourier transform  $F: \mathbb{T}^{m-1} \rightarrow \mathbb{C}$ . After obtaining a pointwise bound on  $F$ , we integrate around that torus to obtain, for sufficiently large  $k$  and  $I = (k^{1-\beta}, k]$ , that  $|S(I, M_1, \dots, M_m)| \gg k^{m-1}$  and lies in the cube  $[-ck, ck]^{m-1}$  for some  $c > 0$ . The density of these sets is sufficiently high that if we look in a larger interval, with positive probability we can find  $j_1, \dots, j_m \in (k, Dk]$  such that  $X_{j_1}^{(1)}, \dots, X_{j_m}^{(m)} > 0$  and

$$(j_m - j_1, \dots, j_m - j_{m-1}) \in S(I; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}).$$

Combining this with the corresponding point in the set of differences then produces a number in  $\mathcal{L}(\mathbf{X}^{(1)}) \cap \dots \cap \mathcal{L}(\mathbf{X}^{(m)})$  made solely from values in  $(k^{1-\beta}, Dk]$  for some constants  $\beta, D > 0$ . By partitioning  $\mathbb{N}$  into infinitely many disjoint sets of this form and repeating this argument for each of them, we conclude that the set of intersections is almost surely infinite.

**1.5. Further questions.** There is still much to be done for both components of this paper—random permutations and random sumsets. Recall that Theorem 1 and Theorem 6 do not pin down the exact behavior at points of discontinuity of  $h$ . A glaring question is to characterize  $m_\alpha$  and  $s_\alpha$  at these points. We are doubtful our approach generalizes. Characterizing the behavior at the critical values is likely difficult, and will require a new idea.

**Question 1.** *What are  $m_\alpha$  and  $s_\alpha$  at discontinuity points of  $h$ ?*

For random permutations we would like a more complete characterization than in Corollary 2. In particular an upper bound.

**Question 2.** *Show that if a permutations has cycle counts that are asymptotically dominated by Poisson random variables with mean  $h^{-1}(2)/k$ , then two will invariably generate  $S_n$  with positive probability.*

Corollary 2 shows that for many permutation measures no finite number will invariably generate  $S_n$ . Possibly if we let the number of permutations grow with  $n$  we will see different behavior.

**Question 3.** *Let  $\alpha > 1/\log 2$ . Prove that there are constants  $\beta < \beta'$  such that the probability  $\beta \log n$  Ewens- $\alpha$  permutations generate  $S_n$  is bounded away from 0, while  $\beta' \log n$  fail to generate  $S_n$  with high probability?*

We believe that  $\log n$  is the correct order by the following approximation model. When  $\alpha > 1/\log 2$  the fixed set sizes in a random permutation are dense in  $[n]$ . So, we can model the occurrence of each fixed size by independent Bernoulli random variables with some parameter  $p_\alpha > 0$ . If one performs  $N$  independent thinnings of  $[n]$  by including each integer  $k$  with probability  $p_\alpha$ , then the probability  $k$  belongs to all  $N$  subsets is  $p_\alpha^N$ . Hence, the probability there are no common elements in the  $N$ -fold intersection is  $(1 - p_\alpha^N)^n$ . If we choose  $N = c \log n$  this will converge to either 0 or a positive number as we increase  $c$ . The difficulty in answering the question for permutations is we do not have independence for fixing different fixed set sizes.

We also have a question in the simpler setting of generating  $S_n$ . Dixon's theorem [Dix92] implies that two uniformly random permutations will generate either  $A_n$  or  $S_n$  with high probability. Does the analogue hold for  $\text{ESF}(\alpha, n)$  permutations? Because generation relies on more than just cycle structure, this may be a hard question.

**Question 4.** *How many  $\text{ESF}(\alpha, n)$  permutations are needed to generate one of  $A_n$  or  $S_n$  with high probability?*

**1.6. Notation.** Note that  $\alpha > 0$  is fixed throughout. As already discussed, we denote cycle counts of a permutation by  $\mathbf{C} = (C_1, \dots, C_n)$  with  $C_j$  the number of  $j$ -cycles. Unless otherwise noted, our permutations and cycle vectors come from an  $\text{ESF}(\alpha, n)$  distribution. We will let  $\mathbf{Y}(\alpha)$  denote a vector of independent  $\text{Poi}(\alpha/k)$  random variables that are obtained from the Feller coupling in (8). We will also take  $\mathbf{X}(\alpha)$  to be a vector of independent  $\text{Poi}(\alpha/k)$  random variables. This is done to distinguish the permutation and random sumset settings. Henceforth we will suppress the  $\alpha$  dependence unless there is reason to call attention to it. For an infinite vector, such as  $\mathbf{Y}$ , we will use the notation  $\mathbf{Y}[i, j]$  to denote the sub-vector  $(Y_i, Y_{i+1}, \dots, Y_j)$ .

For  $I$  an interval in  $\mathbb{N}$  define the sumset

$$\mathcal{L}(I, \mathbf{X}) := \left\{ \sum_{j \in I} j x_j : 0 \leq x_j \leq X_j \right\},$$

and set  $\mathcal{L}(\mathbf{X}) := \mathcal{L}(\mathbb{N}, \mathbf{X})$ . Given  $\mathbf{X}$  define

$$(5) \quad f_{\ell, k}(\mathbf{X}) = \sum_{\ell < j \leq k} X_j, \quad g_{\ell, k}(\mathbf{X}) = \sum_{\ell < j \leq k} j X_j.$$

It will be convenient to abbreviate  $f_k := f_{1, k}(\mathbf{X})$  and  $g_k := g_{1, k}(\mathbf{X})$ . Thus,  $f_k$  is the number of available summands smaller than  $k$ , and  $g_k$  is the largest sum attainable with them.



We will use the notation  $f \ll g$  and  $f(n) = O(g(n))$  interchangeably for the existence of  $c$  such that for all large enough  $n$  it holds that  $f(n) \leq cg(n)$ . When the  $c$  depends on our choice of  $\varepsilon$  we will use  $f \ll_\varepsilon g$ , similarly  $f \ll_{m,\varepsilon} g$  denotes dependence of the constant on both  $\varepsilon$  and the number of intersections  $m$ . We use the little- $o$  notation  $f(n) = o(g(n))$  to mean that  $f(n)/g(n) \rightarrow 0$ . Also,  $f(n) = \tilde{O}(g(n))$  means there is  $k > 0$  such that  $f(n) = O(\log^k(n)g(n))$ . The symbol  $f(n) \approx g(n)$  means that  $f(n)/g(n) \rightarrow c$  for some  $c > 0$ . A sequence of events  $E_n$  occurs *with high probability* if  $\liminf \mathbf{P}[E_n] = 1$ . Also  $i \mid j$  means that  $i$  divides  $j$  (i.e. there is an integer  $k$  with  $ik = j$ .)

**1.7. Outline of paper.** We will lead off with a proof of Theorem 1. This comes in two parts: an upper bound from Theorem 6, and a matching lower bound in Proposition 9. The upper bound in Theorem 6 has two distinct components. We connect random sumsets to  $\text{ESF}(\alpha, n)$  permutations in Section 3.1. This section includes the proofs of Theorem 3, Theorem 4, and Theorem 5. The second component is analyzing the random sumset model. We do this in Section 4 and provide an upper bound on  $s_\alpha$  at Proposition 23. The lower bound is Proposition 9 and proven in Section 5.

**1.8. Acknowledgements.** We would like to thank Robin Pemantle for several helpful conversations. We are very grateful for Richard Arratia's correspondence. He made us aware of the indispensable Feller coupling. Also, thanks to Clayton Barnes, Emily Dinan, and Jacob Richey for their assistance in the formative stages of this project.

## 2. PROOF OF THEOREM 1

First we show that  $h(\alpha) + 1$  is an upper bound for the number of  $\text{ESF}(\alpha, n)$  permutations to invariably generate  $S_n$ .

**Proposition 7.** *Suppose  $\alpha$  is a continuity point of  $h$ . A collection of  $h(\alpha)$  independent permutations sampled according to an  $\text{ESF}(\alpha, n)$  invariably generates  $S_n$  with positive probability as  $n \rightarrow \infty$ .*

*Proof.* Let  $m = h(\alpha)$ . Call the permutations  $\pi^{(1)}, \dots, \pi^{(m)}$ . Condition  $\pi^{(1)}$  to be odd. Lemma 19 guarantees this happens with probability bounded away from zero. Define the events

$$\begin{aligned} E_{n,k} &= \{\pi^{(1)}, \dots, \pi^{(m)} \text{ fix an } \ell\text{-set for some } k \leq \ell \leq n/2\}, \\ F_{n,k} &= \{\pi^{(2)} \text{ has no } \ell\text{-cycles with } \ell \leq k\}. \end{aligned}$$

The probability of a common fixed set size amongst all of the permutations is bounded above by

$$(6) \quad \mathbf{P}[E_{n,k} \cup F_{n,k}^c] \leq \mathbf{P}[E_{n,k}] + \mathbf{P}[F_{n,k}^c].$$

Therefore, the  $\pi^{(i)}$  will invariably generate a transitive subgroup of  $S_n$  if this quantity is less than 1.

Now  $\alpha$  is a continuity point of  $h$ , so

$$m = h(\alpha) = \lceil (1 - \alpha \log 2)^{-1} \rceil > (1 - \alpha \log 2)^{-1}.$$

It follows that there exists some  $\varepsilon > 0$  such that

$$m = (1 - (\alpha + \varepsilon) \log 2)^{-1}.$$

Fix  $\varepsilon'$  such that  $0 < \varepsilon' < \varepsilon$ . By Lemma 18 for any  $k$  and  $i = 2, \dots, m$ ,

$$\mathbf{P}[\pi^{(i)} \text{ fixes a } k\text{-set}] \leq ck^{-\delta},$$

where

$$\delta = 1 - (\alpha + \varepsilon') \log 2.$$

Similarly, by Corollary 21 for any  $k$ ,

$$\mathbf{P}[\pi^{(1)} \text{ fixes a } k\text{-set}] \leq ck^{-\delta} \cdot \max \left\{ \frac{\alpha + 1}{\alpha}, \frac{\alpha + 1}{1} \right\}.$$

By independence of the  $\pi^{(i)}$ , we conclude

$$\mathbf{P}[E_{n,k}] \leq (ck^{-\delta})^m \cdot \max \left\{ \frac{\alpha + 1}{\alpha}, \frac{\alpha + 1}{1} \right\}.$$

By construction we have that  $\delta m > 1$ . A union bound for  $k_0 \leq k \leq n/2$  ensures that, given some  $\beta > 0$ , we can choose  $k_0$  such that  $\mathbf{P}[E_{n,k_0}] < \beta$ . Moreover, [ABT00, Theorem 3.1] ensures that the cycle counts  $\mathbf{C}[1, k_0]$  of  $\pi_n^{(2)}$  converge in total variation to  $\mathbf{Y}[1, k_0]$ . Hence,

$$\liminf_{n \rightarrow \infty} \mathbf{P}[F_{n,k_0}] > 0.$$

Set  $\beta$  equal to half this limit infimum. Now, for an appropriate  $k_0$  and large enough  $n$ , it holds that (6) is strictly less than 1. This means that with positive probability the collection invariably generates a transitive subgroup of  $S_n$ . By Theorem 3 we know this transitive subgroup is with high probability either  $A_n$  or  $S_n$ . Because  $\pi^{(1)}$  is odd, it must be  $S_n$ .  $\square$

*Remark 8.* The argument above implies that  $m_\alpha \leq m_{\alpha+\eta}$  for all  $\eta > 0$ , since any appropriate choice of  $\varepsilon'$  in the latter case will hold for the former. It follows that  $h(\alpha) + 1$  permutations will invariably generate with positive probability at discontinuity points of  $h$ .

Now we prove a matching lower bound.

**Proposition 9.** *A collection of  $m < h(\alpha)$  permutations sampled independently according to an  $\text{ESF}(\alpha, n)$  with high probability do not invariably generate  $S_n$ , or any transitive subgroup of  $S_n$ .*

*Proof.* Let  $m < h(\alpha)$ , and fix some  $\varepsilon > 0$ . By Proposition 24 the intersection of the i.i.d. sumsets with parameter  $\alpha$ ,  $\bigcap_{i=1}^m \mathcal{L}(\mathbf{X}^{(i)})$ , is almost surely infinite. It follows that there is some  $k_0 = k_0(\varepsilon)$  such that if  $k \geq k_0$  then  $\bigcap_{i=1}^m \mathcal{L}(\mathbf{X}^{(i)}) \cap [1, k] \neq \emptyset$  with probability at least  $1 - \varepsilon/2$ .

Fix some  $k \geq k_0$  and call the random permutations  $\pi^{(1)}, \dots, \pi^{(m)}$ . By [ABT00, Theorem 3.1] the cycle counts  $\mathbf{C}^{(i)}[1, k]$  of  $\pi^{(i)}$  converge in total variation to  $\mathbf{X}^{(i)} \cap [1, k]$ . Then there exists some  $n_0 = n_0(\varepsilon, k)$  such that if  $n \geq n_0$ , with probability greater than  $1 - \varepsilon/2$  we have  $\mathbf{C}^{(i)}[1, k] = \mathbf{X}^{(i)} \cap [1, k]$  for all  $i = 1, \dots, m$ . Since

$$\bigcap_{i=1}^m \mathcal{L}(\mathbf{X}^{(i)}) \cap [1, k] \subset \bigcap_{i=1}^m \mathcal{L}(\mathbf{X}^{(i)} \cap [1, k]),$$

with probability at least  $1 - \varepsilon$  we have that  $\pi^{(1)}, \dots, \pi^{(m)}$  each fix a set of size  $\ell$  for some  $\ell \leq k$ . As  $\varepsilon$  was arbitrary, this completes our proof.  $\square$

Theorem 1 is a straightforward consequence of the last two propositions.

*Proof of Theorem 1.* Together [ABT00, Theorem 3.1, Theorem 3.2] guarantee that the cycle counts of any measure satisfying the strong  $\alpha$ -logarithmic property converge in total variation to the same distribution as an  $\text{ESF}(\alpha, n)$  permutation. Hence it suffices to consider  $\text{ESF}(\alpha, n)$  permutations.

By Proposition 7 we have  $m_\alpha \leq h(\alpha)$  at point of continuity of  $h$ . At points of discontinuity, we use Remark 8 to deduce that  $m_\alpha \leq m_{\alpha+\eta} \leq h(\alpha) + 1$ . Then, by Proposition 9 we have that  $h(\alpha) \leq m_\alpha$  for all  $\alpha$ , completing our proof.  $\square$

### 3. THE UPPER BOUND FOR $m_\alpha$

The main goal of this section is to prove that  $m_\alpha \leq s_\alpha$ . Our primary tool for relating Poisson sumsets to permutations is the Feller coupling. This is described at the onset of Section 3.1. We then use it in that section to prove several estimates on the cycle structure of  $ESF(\alpha, n)$  permutations. With these we prove Theorem 3, Theorem 4, and Theorem 5 in Section 3.2. We put all of this together and establish Proposition 7 in Section 3.3.

**3.1. The Feller Coupling.** The Ewens sampling formula can be obtained via an elegant coupling attributed to Feller [Fel45, p. 815] for uniform permutations. The articles [ABT92, ABT16] have nice descriptions. We start with a sequence  $\xi_1, \xi_2, \dots$  of mixed Bernoulli random variables with  $\mathbf{P}[\xi_i = 1] = \frac{\alpha}{\alpha+i-1}$  and  $\mathbf{P}[\xi_i = 0] = \frac{i-1}{\alpha+i-1}$ . Define an  $\ell$ -spacing to be any occurrence of  $\ell - 1$  zeros enclosed by a 1 on the left and right (e.g. 1, 0, 0, 0, 1 is a 4 spacing). Remarkably, the total number of  $\ell$ -spacings,  $Y_\ell$ , is distributed as  $\text{Poi}(\alpha/\ell)$ . Moreover, the collection  $Y_1, Y_2, \dots$  are independent (see [ABT16, ABT92]).

The counts of spacings in  $\xi_1, \dots, \xi_n, 1$  generate a partition of  $n$ , which can be filled in uniformly randomly to form a permutation with  $C_\ell$  cycles of size  $\ell$ , where  $C_\ell$  are sampled according to an  $ESF(\alpha, n)$  distribution. Explicitly,

$$\begin{aligned} C_\ell &= \text{the number of } \ell\text{-spacings in } \xi_1, \dots, \xi_n, 1 \\ (7) \quad &= \xi_{n-\ell+1}(1 - \xi_{n-\ell+2}) \cdots (1 - \xi_n) + \sum_{k=1}^{n-\ell} \xi_k(1 - \xi_{k+1}) \cdots (1 - \xi_{k+\ell-1})\xi_{k+\ell}. \end{aligned}$$

This gives an intuition for why  $ESF(1, n)$  corresponds to a uniformly random permutation. Indeed, we can inductively construct such a permutation by letting  $\xi_i$  indicate the decision to complete a cycle, when there is an  $i$ -way choice for the next element.

Letting  $R_n$  be the index of the rightmost 1 in  $\xi_1, \dots, \xi_n$  and  $J_n = n + 1 - R_n$  it follows from the previous discussion that

$$(8) \quad C_\ell \leq Y_\ell + \mathbf{1}\{J_n = \ell\}.$$

This says that the cycle counts can be obtained from independent Poisson random variables through a random number of deletions, and possibly one insertion. We require a few estimates on the behavior of these perturbations.

**Lemma 10.** *Let  $J_n$  be as defined above, and  $D_n = \sum_{\ell=1}^n Y_\ell - \mathbf{1}\{J_n = \ell\} - C_\ell$  be the number of deletions. The following four inequalities hold:*

$$(9) \quad \mathbf{P}[J_n = \ell] \leq \frac{\alpha}{n - \ell}, \quad \ell < n.$$

$$(10) \quad \mathbf{P}[J_n = \ell] \leq cn^{-\alpha(1-\gamma)}, \quad n - n^\gamma < \ell < n, \quad 0 < \gamma < 1, \text{ for some } c = c(\gamma) > 0.$$

$$(11) \quad \mathbf{P}[J_n = \ell] = O(n^{-\alpha/(1+\alpha)}), \quad \ell < n.$$

$$(12) \quad \mathbf{E}D_n = O(1).$$

*Proof.* The inequality in (9) follows from the formula given in [ABT92, Remark following (17)], which says  $\mathbf{P}[J_n = \ell] = \ell \mathbf{E}C_\ell^{(n)}/n$ . The coupling at (8) ensures that  $\mathbf{P}[J_n = \ell] \leq (\alpha + \ell \mathbf{P}[J_n = \ell])/n$ . Solving for  $\mathbf{P}[J_n = \ell]$  gives (9).

Fix some  $\gamma \in (0, 1)$ . For the case  $\ell > n - n^\gamma$  in (10) we use that when  $J_n = \ell$  we must have  $\xi_{n-\ell+1} = 1$  and  $\xi_k = 0$  for all larger index terms up to  $\xi_n$ . The probability of this can be computed explicitly as

$$\mathbf{P}[J_n = \ell] = \frac{\alpha}{\alpha + n - \ell} \prod_{n-\ell+2}^n \frac{i-1}{\alpha + i - 1} \leq \prod_{n-\ell+1}^n \frac{i-1}{\alpha + i - 1}.$$

We estimate the product by converting it to a sum

$$\prod_{n-\ell+1}^n \frac{i-1}{\alpha + i - 1} = \exp\left(-\sum_{n-\ell+1}^n \log \frac{\alpha + i - 1}{i - 1}\right) \leq \exp\left(-\int_{n-\ell+1}^n \log \frac{\alpha + x - 1}{x - 1} dx\right).$$

The last inequality follows from the fact that  $\log \frac{\alpha+x-1}{x-1}$  is a decreasing function, and the sum can be viewed as a right-sided Riemann (over-)approximation. This integral has a closed form

$$-\int_{n-\ell+1}^n \log\left(\frac{\alpha + x - 1}{x - 1}\right) dx = -\log\left(\frac{(\alpha + n - 1)^{\alpha+n-1}}{(n-1)^{n-1}}\right) + \log\left(\frac{(\alpha + n - \ell)^{\alpha+n-\ell}}{(n-\ell)^{n-\ell}}\right).$$

Hence, exponentiating the above line gives

$$(13) \quad \prod_{n-\ell+1}^n \frac{i-1}{\alpha + i - 1} \leq \frac{(n-1)^{n-1}}{(\alpha + n - 1)^{\alpha+n-1}} \times \frac{(\alpha + n - \ell)^{\alpha+n-\ell}}{(n-\ell-1)^{n-\ell}}.$$

The leftmost product is less than  $n^{-\alpha}$ . The rightmost product can be written as

$$(14) \quad (\alpha + n - \ell)^\alpha \left(\frac{n - \ell + \alpha}{n - \ell - 1}\right)^{n-\ell} = (\alpha + n - \ell)^\alpha \left(\frac{1 + \frac{\alpha}{n-\ell}}{1 - \frac{1}{n-\ell}}\right)^{n-\ell}.$$

The rightmost product in (14) is asymptotic to  $e^\alpha/e^{-1}$  as  $n - \ell \rightarrow \infty$ , and thus may be bounded by some constant for all values of  $n - \ell$ . Using the hypothesis that  $n - \ell \leq n^\gamma$ , it follows that (14) is universally bounded by  $cn^{\alpha\gamma}$  for some constant  $c$ . We conclude that (13) is less than  $cn^{-\alpha+\alpha\gamma} = cn^{-\alpha(1-\gamma)}$ . This establishes (10).

To obtain the universal bound at (11), observe when  $\ell \leq n - n^{\alpha/(1+\alpha)}$  we can input this into (9) to obtain

$$\mathbf{P}[J_n = \ell] \leq \frac{\alpha}{n - (n - n^{\alpha/(1+\alpha)})} = O(n^{-\alpha/(1+\alpha)}).$$

And, for  $\ell > n - n^\alpha$  we substitute  $\gamma = \alpha/(1 + \alpha)$  into (10) to obtain the same asymptotic inequality:  $O(n^{-\alpha/(1+\alpha)})$ .

Lastly, (12) is proven in [ABT92, Theorem 2].  $\square$

We will also require a bound on the joint probability that two cycles occur simultaneously. There will be some poly-log terms that, besides being a minor nuisance, do not effect the tack of our proof. Recall the  $\tilde{O}$  notation that ignores logarithmic contribution. It is described carefully in Section 1.6.

**Lemma 11.** *For any  $i < j \leq n$  it holds that*

$$\mathbf{P}[C_i C_j > 0] = \tilde{O}(i^{-1} j^{-\alpha/(1+\alpha)}).$$

*Proof.* We start by using the formula at (7) to bound  $C_i$  with the  $\xi_k$ ,

$$C_i \leq \xi_{n-i+1}(1 - \xi_{n-i+2}) \cdots (1 - \xi_n) + \sum_{k=1}^{n-i} \xi_k \xi_{k+i}.$$

Thus,

$$\begin{aligned} C_i C_j &\leq \left( \xi_{n-i+1}(1 - \xi_{n-i+2}) \cdots (1 - \xi_n) + \sum_{k=1}^{n-i} \xi_k \xi_{k+i} \right) \\ &\quad \times \left( \xi_{n-j+1}(1 - \xi_{n-j+2}) \cdots (1 - \xi_n) + \sum_{\ell=1}^{n-j} \xi_\ell \xi_{\ell+j} \right) \\ &= (x + y)(z + w). \end{aligned}$$

The last line is just labeling the terms in the product immediately above in the natural way (i.e.  $y = \sum_{k=1}^{n-i} \xi_k \xi_{k+i}$ ). This is so we can bound  $\mathbf{E}[xz + xw + yw + yz]$  in an organized fashion, one term at a time.

**Term  $xz$ :** First, consider  $\xi_{n-i+1}(1 - \xi_{n-i+2}) \cdots (1 - \xi_n) \xi_{n-j+1}(1 - \xi_{n-j+2}) \cdots (1 - \xi_n)$ . When  $i < j$  this product contains the term  $\xi_{n-i+1}(1 - \xi_{n-i+1}) \equiv 0$ , thus it is always zero. We conclude that

$$(15) \quad \mathbf{E}[xz] \equiv 0.$$

**Term  $xw$ :** Next, we consider the cross-term  $\xi_{n-i+1}(1 - \xi_{n-i+2}) \cdots (1 - \xi_n) \sum_{\ell=1}^{n-j} \xi_\ell \xi_{\ell+j}$ . Many of the summands are zero. In fact, the overlapping terms with  $n - j - i + 1 < \ell \leq n - j$  are identically zero. So, for the sake of obtaining disjoint terms, we consider the smaller sum

$$\xi_{n-i+1}(1 - \xi_{n-i+2}) \cdots (1 - \xi_n) \sum_{\ell=1}^{n-j-i+1} \xi_\ell \xi_{\ell+j}.$$

Aside from the  $\ell = n - j - i + 1$  term, all the indices are all disjoint. Ignoring this term for now, the expected value is

$$(16) \quad \frac{\alpha}{\alpha + n - i} \frac{n - i + 1}{\alpha + n - i + 1} \cdots \frac{n - 1}{\alpha + n - 1} \sum_{\ell=1}^{n-j-i} \frac{\alpha^2}{(\alpha + \ell - 1)(\alpha + \ell - 1 + j)}.$$

Now  $i$  and  $j$  correspond to cycle lengths, so we must have  $i + j \leq n$  to have a nonzero expectation at all. Since  $i < j$  we conclude that  $i < n/2$ . A simple bound

on the product outside the sum is to plug this value into the first term and ignore the rest. This gives the bound

$$\frac{\alpha}{\alpha+n-i} \frac{n-i+1}{\alpha+n-i+1} \cdots \frac{n-1}{\alpha+n-1} < \frac{\alpha}{n-(n/2)+1} < \frac{2\alpha}{n}.$$

Ignoring the product outside of it, the sum can be compared to the integral  $\int_1^n \frac{1}{x(x+j)} dx$  to prove it is  $O(\log(j)/j)$ . Thus the expression in (16) is  $\tilde{O}(1/nj)$ .

Rather than using the rough bound from above, the full  $\ell = n-j-i+1$  term is

$$\xi_{n-j-i+1}(1-\xi_{n-j-i+2}) \cdots (1-\xi_{n-i}) \xi_{n-i+1}^2 (1-\xi_{n-i+2}) \cdots (1-\xi_n).$$

The expectation of this term is

$$\frac{\alpha}{\alpha+n-j-i} \left( \prod_{k=n-j-i+2}^{n-i} \frac{k-1}{\alpha+k-1} \right) \frac{\alpha}{\alpha+n-i} \left( \prod_{k=n-i+2}^n \frac{k-1}{\alpha+k-1} \right).$$

But this is just

$$\begin{aligned} \frac{\alpha}{\alpha+n-i} \frac{\alpha+n-i}{n-i} \mathbf{P}[J_n = j+i] &= \frac{\alpha}{n-i} \mathbf{P}[J_n = j+i] \\ &\leq \frac{2\alpha}{n} \mathbf{P}[J_n = j+i]. \end{aligned}$$

Then by Lemma 10 (11) we have the bound

$$\mathbf{P}[J_n = j+i] = O(n^{-\alpha/(1+\alpha)}).$$

Thus this term is  $O(i^{-1}j^{-\alpha/(1+\alpha)})$ , and

$$(17) \quad \mathbf{E}[xw] = \tilde{O}(i^{-1}j^{-\alpha/(1+\alpha)}).$$

**Term  $yw$ :** Because  $i < j$  the term  $\xi_{n-j+1}(1-\xi_{n-j+2}) \cdots (1-\xi_n) \sum_{\ell=1}^{n-i} \xi_\ell \xi_{\ell+i}$  behaves differently than the case just prior. In fact, it is the largest order term amongst the four. The first step is the same as before though. A few of the terms are identically zero. So, we can write  $yw$  as

$$\xi_{n-j+1}(1-\xi_{n-j+2}) \cdots (1-\xi_n) \sum_{\ell=1}^{n-i-j+1} \xi_\ell \xi_{\ell+i}.$$

Except for when  $\ell = n-i-j+1$ , all of the indices now disjoint. When we take expectation of the terms with disjoint indices we obtain

$$\frac{\alpha}{\alpha+n-j} \frac{n-j+1}{\alpha+n-j+1} \cdots \frac{n-1}{\alpha+n-1} \sum_{\ell=1}^{n-j-i} \frac{\alpha^2}{(\alpha+\ell-1)(\alpha+\ell+i-1)}.$$

Notice that  $j$  could be quite large. The best bound we have for the product outside the sum comes from (11). This implies it is  $O(n^{-\alpha/(1+\alpha)})$ . As with (16), the sum term is  $O(\log i/i)$ . This yields that the whole expression is  $\tilde{O}(i^{-1}j^{-\alpha/(1+\alpha)})$ .

As before, the full  $\ell = n-i-j+1$  term is

$$\xi_{n-i-j+1}(1-\xi_{n-j-i+2}) \cdots (1-\xi_{n-j}) \xi_{n-j+1}^2 (1-\xi_{n-i+2}) \cdots (1-\xi_n).$$

The expectation of this term is

$$\frac{\alpha}{\alpha+n-j-i} \left( \prod_{k=n-j-i+2}^{n-j} \frac{k-1}{\alpha+k-1} \right) \frac{\alpha}{\alpha+n-i} \left( \prod_{k=n-j+2}^n \frac{k-1}{\alpha+k-1} \right).$$

This simplifies to

$$\frac{\alpha}{\alpha + n - j} \frac{\alpha + n - j}{n - j} \mathbf{P}[J_n = j + i] = \frac{\alpha}{n - j} \mathbf{P}[J_n = j + i].$$

By construction  $i \leq n - j$ , and again by Lemma 10 (11), we have that  $\mathbf{P}[J_n = j + i] = O(n^{-\alpha/(1+\alpha)})$ . Thus this term has expectation that is  $O(i^{-1}j^{-\alpha/(1+\alpha)})$ . It follows that

$$(18) \quad \mathbf{E}[yw] = \tilde{O}(i^{-1}n^{-\alpha/(1+\alpha)}).$$

**Term  $yz$ :** The last step is to bound the product

$$(19) \quad \left( \sum_{k=1}^{n-i} \xi_k \xi_{k+i} \right) \left( \sum_{\ell=1}^{n-j} \xi_\ell \xi_{\ell+j} \right) = \sum_{k,\ell=1}^{n-i,n-j} \xi_k \xi_{k+i} \xi_\ell \xi_{\ell+j}.$$

Call the index set  $\Lambda = \{(k, \ell) : k \in [1, \dots, n-i], \ell \in [1, \dots, n-j]\}$ . As  $i < j$ , we can divide  $\Lambda$  into disjoint sets

$$\begin{aligned} \Lambda_0 &= \{k, k+i, \ell, \text{ and } \ell+j \text{ are all distinct}\}, \\ \Lambda_1 &= \{k = \ell\}, \\ \Lambda_2 &= \{k = \ell + j\}, \\ \Lambda_3 &= \{k + i = \ell\}, \\ \Lambda_4 &= \{k + i = \ell + j\}. \end{aligned}$$

This yields the following upper bound on (19):

$$\sum_{\Lambda_0} \xi_k \xi_{k+i} \xi_\ell \xi_{\ell+j} + \sum_{\Lambda_1} \xi_k \xi_{k+i} \xi_{\ell+j} + \sum_{\Lambda_2} \xi_k \xi_{k+i} \xi_\ell + \sum_{\Lambda_3} \xi_k \xi_{k+i} \xi_{\ell+j} + \sum_{\Lambda_4} \xi_k \xi_{k+i} \xi_\ell.$$

The payoff of this partition is that each product of  $\xi$  above is of distinct, independent terms. This lets us tidily compute the expectation of each. For  $(k, \ell) \in \Lambda_0$  we have the  $k, k+i, \ell, \ell+j$  are all distinct. This gives

$$\mathbf{E}[\xi_k \xi_{k+i} \xi_\ell \xi_{\ell+j}] \leq \frac{A}{k(k+i)\ell(\ell+j)}$$

for some constant  $A$  depending only on  $\alpha$ . We can take the expectation of the entire sum

$$\mathbf{E} \sum_{\Lambda_0} \xi_k \xi_{k+i} \xi_\ell \xi_{\ell+j} \leq \sum_{k=1, \ell=1}^n \mathbf{E}[\xi_k \xi_{k+i} \xi_{\ell+j}] \leq \sum_{k=1, \ell=1}^n \frac{A}{k(k+i)\ell(\ell+j)} = \tilde{O}(1/ij).$$

We can parametrize  $\Lambda_1$  by  $k$  to write it as  $\Lambda_1 = \{(k, k) : k = 1, \dots, n-j\}$ , this gives the bound

$$\mathbf{E} \sum_{\Lambda_1} \xi_k \xi_{k+i} \xi_{\ell+j} \leq \sum_{k=1}^n \mathbf{E}[\xi_k \xi_{k+i} \xi_{k+j}] \leq \sum_{k=1}^n \frac{A}{k(k+i)(k+j)} = \tilde{O}(1/ij).$$

We can similarly parametrize the sums over  $\Lambda_2, \Lambda_3$  and  $\Lambda_4$  to obtain

$$(20) \quad \mathbf{E}[yz] = \tilde{O}(1/ij)$$

All of the expressions at (15), (17), (18), and (20) are  $\tilde{O}(i^{-1}j^{-\alpha/(1+\alpha)})$ . Markov's inequality yields

$$(21) \quad \mathbf{P}[C_i C_j > 0] = \tilde{O}(i^{-1}j^{-\alpha/(1+\alpha)}).$$

This proves the claimed inequality.  $\square$

We also need a bound on the probability that cycles of the same size occur.

**Lemma 12.** *For any  $i \leq n$  it holds that*

$$\mathbf{P}[C_i \geq 2] = \tilde{O}(i^{-2} + n^{-1-\alpha/(1+\alpha)}).$$

*Proof.* We start by bounding  $\mathbf{P}[C_i > 2]$ . By (8) we have

$$(22) \quad \mathbf{P}[Y_i + \mathbf{1}\{J_n = i\} > 2] \leq \mathbf{P}[Y_i > 1] = O(1/i^2).$$

It remains to bound  $\mathbf{P}[C_i = 2]$ . Conditioning on the value of  $J_n$ , we obtain the decomposition

$$(23) \quad \mathbf{P}[C_i = 2] = \mathbf{P}[C_i = 2 \mid J_n = i] \mathbf{P}[J_n = i] + \mathbf{P}[C_i = 2 \mid J_n \neq i] \mathbf{P}[J_n \neq i].$$

First we estimate the first summand on the right hand side of (23). Because two cycles larger than  $n/2$  cannot occur, we must have  $i \leq n/2$ . Then by Lemma 10 (9),  $\mathbf{P}[J_n = i] \leq 2\alpha/n$ . When  $J_n = i$ , it ensures that the sequence  $\xi_1, \dots, \xi_n$  has  $\xi_{n-i+1} = 1$  and the larger index  $\xi_k$  are zero. The smaller index  $\xi_i$  are independent of this event. The value of  $C_i$  conditioned on  $J_n = i$  is thus one more than the number of  $i$ -spacings in the sequence

$$\xi_1, \dots, \xi_{n-i}, 1,$$

with  $\xi_1, \dots, \xi_{n-i}$  independent and distributed  $ESF(\alpha, n-i)$ . Call the number of  $i$ -spacings in the above sequence  $C_i^-$ . So, conditional on  $J_n = i$  we have  $C_i = C_i^- + 1$ . By writing explicitly what it means for an  $i$ -spacing to arise, we can bound  $C_i^-$  in terms of the  $\xi_k$ :

$$C_i^- \leq \xi_{n-2i+1}(1 - \xi_{n-2i+2}) \cdots (1 - \xi_{n-i}) + \sum_{k=1}^{n-2i} \xi_k \xi_{k+i}.$$

Looking to apply Markov's inequality, we take the expectation of the above line and obtain

$$\mathbf{E}C_i^- \leq \frac{\alpha}{\alpha + n - 2i} \frac{n - 2i + 1}{\alpha + n - 2i + 1} \cdots \frac{n - i - 1}{\alpha + n - i - 1} + \sum_{k=1}^{n-2i} \frac{\alpha^2}{(\alpha + k - 1)(\alpha + k - 1 + i)}.$$

The product above is equivalent to  $\mathbf{P}[J_{n-i} = i]$ , then we use Lemma 10 (11) and the fact that  $i < n/2$  to bound it by  $\tilde{O}((n-i)^{-\alpha/(1+\alpha)}) = \tilde{O}(n^{-\alpha/(1+\alpha)})$ . The sum, as we have seen from (16), has order  $\tilde{O}(1/i)$ . Recalling that (9) implies  $\mathbf{P}[J_n = i] = O(1/n)$ , it follows that

$$(24) \quad \mathbf{P}[C_i = 2 \mid J_n = i] \mathbf{P}[J_n = i] = \tilde{O}(n^{-1-\alpha/(1+\alpha)} + 1/in) = \tilde{O}(i^{-2} + n^{-1-\alpha/(1+\alpha)}).$$

Now we estimate the second summand on the right hand side of (23). Under the event  $\{J_n \neq i\}$ , for  $C_i$  to equal 2, it is necessary that two  $i$ -spacings occur in the infinite sequence  $\xi_1, \xi_2, \dots$ . The count of  $i$ -spacings is distributed as  $Y_i$  from (8). Therefore,

$$(25) \quad \mathbf{P}[C_i = 2 \text{ and } J_n \neq i] \leq \mathbf{P}[Y_i \geq 2] = O(1/i^2).$$

Then (22), (24), and (25) imply that

$$(26) \quad \mathbf{P}[C_i \geq 2] = \tilde{O}(i^{-2} + n^{-1-\alpha/(1+\alpha)})$$

as desired.  $\square$

Using the previous two lemmas we may prove the following.



**Proposition 13.** *Let  $\pi \sim \text{ESF}(\alpha, n)$  and  $a = 1 - \frac{\alpha}{4\alpha+3}$ . The probability that  $\pi$  has two cycles whose lengths have a common divisor larger than  $n^a$  is  $o(1)$ .*

*Proof.* Call  $E_a$  the event that  $\pi$  has two cycles with common divisor larger than  $n^a$ . We utilize a union bound, then apply Lemma 11 and Lemma 12 to write

$$\begin{aligned} \mathbf{P}[E_a] &\leq \sum_{d=\lceil n^a \rceil}^n \left( \sum_{1 \leq i < j}^{\lfloor n^{1-a} \rfloor} \mathbf{P}[C_{id}C_{jd} > 0] + \sum_{i=1}^{\lfloor n^{1-a} \rfloor} \mathbf{P}[C_{id} \geq 2] \right) \\ &= \tilde{O} \left( \sum_{d=\lceil n^a \rceil}^n \sum_{1 \leq i < j}^{\lfloor n^{1-a} \rfloor} (id)^{-1}(jd)^{-\alpha/(1+\alpha)} + \sum_{d=\lceil n^a \rceil}^n \sum_{i=1}^{\lfloor n^{1-a} \rfloor} \left( \frac{1}{(id)^2} + n^{-1-\alpha/(1+\alpha)} \right) \right). \end{aligned}$$

Since  $d \geq n^a$  the above line is

$$\tilde{O} \left( n^1 n^{2(1-a)} n^{-a-a\alpha/(1+\alpha)} + n^1 n^{1-a} n^{-2a} + n^{1-a-\alpha/(1+\alpha)} \right).$$

We can simplify the exponents in each term to

$$3 - 3a - a\alpha/(1+\alpha), \quad 2 - 3a, \quad \text{and} \quad 1 - a - \alpha/(1+\alpha),$$

respectively. Some algebra shows that all are negative as long as  $a > 1 - \frac{\alpha}{4\alpha+3}$ . For such  $a$  we have  $\mathbf{P}[E_a] = o(1)$ .  $\square$

**3.2. Proofs of Theorem 3, Theorem 4, and Theorem 5.** We now have enough to establish our bound on the minimal degree of an  $\text{ESF}(\alpha, n)$  permutation.

**Lemma 14.** *Let  $\pi \sim \text{ESF}(\alpha, n)$ . For each  $0 < \beta < 1$ , there exists  $\lambda \in (0, 1)$  such that if we define the set*

$$Q_n = \{d < n^\beta : \text{there exists a prime } p > n^{\lambda\beta} \text{ with } p \mid d\},$$

*then*

$$(27) \quad \mathbf{P}[\exists C_d = 1 \text{ with } d \in Q_n] = 1 - o(1).$$

*Proof.* We start with [ABT00, Theorem 3.1] which implies

$$(28) \quad \sum_{d \in Q_n} C_d \xrightarrow{TV} \text{Poi}(\kappa_n),$$

where

$$\kappa_n = \sum_{d \in Q_n} \frac{\alpha}{d}.$$

Borrowing an argument from [Bov80, p. 50] we have

$$\begin{aligned} \sum_{d \in Q_n} \frac{1}{d} &= \sum_{d < n^\beta} \frac{1}{d} - \sum_{\substack{d < n^\beta \\ p \mid d \Rightarrow p \leq n^{\lambda\beta}}} \frac{1}{d} \\ &\geq \sum_{d < n^\beta} \frac{1}{d} - \prod_{p \leq n^{\lambda\beta}} (1 - 1/p)^{-1} \\ &= \beta \log n - e^{\gamma^*} \lambda \beta \log n + O(1) \end{aligned}$$

where  $\gamma^*$  is Euler's constant. When  $\lambda$  is such that  $e^{\gamma^*} \lambda \beta < \beta/2$  we have  $\lambda_n > \frac{\beta}{2} \log n$  for all  $n$ . It follows from (28) and standard estimates on the concentration of a Poisson random variable that

$$\mathbf{P}\left[\sum_{d \in Q_n} C_d > (\beta/4) \log n\right] \rightarrow \mathbf{P}[\text{Poi}(\lambda_n) > (\beta/4) \log n] = 1 - o(1).$$

To obtain (27), observe that the convergence statement in [ABT00, Theorem 3.1] implies that  $\mathbf{P}[C_d > 1] \rightarrow \mathbf{P}[Y_d > 1] = O(1/d^2)$ . Here  $Y_d$  is a Poisson random variable as in (8). The Borel-Cantelli lemma implies that only finitely many  $Y_d$  are larger than 1. Hence  $\sum_{Y_i > 1} Y_i$  is almost surely bounded. We have seen that, for  $n$  large, the sum of  $C_d$  with  $d \in Q_n$  is at least  $\text{Poi}(\frac{\beta}{4} \log n)$  with probability  $1 - o(1)$ . This diverges, and so one or more of the positive  $C_d$  must be equal to one. Our claim follows.  $\square$

For a random permutation  $\pi \sim \text{ESF}(\alpha, n)$ , we define  $\Phi(\pi) = \prod_{\ell=1}^n \ell^{C_\ell}$ . To prove Theorem 4, it suffices to show that with high probability  $\pi$  has a cycle of length  $d$  such that

$$(29) \quad d \leq n^\beta,$$

$$(30) \quad d^2 \nmid \Phi(\pi).$$

To that end we establish one more lemma.

**Lemma 15.** *Let  $\pi$ ,  $\beta$ ,  $\lambda$ , and  $Q_n$  be as in Lemma 14, then*

$$(31) \quad \mathbf{P}[\exists d \in Q_n \text{ such that } d^2 \nmid \Phi(\pi) \text{ and } C_d = 1] = 1 - o(1).$$

*Proof.* Call the event in (31)  $F_n$ . Conditioning on the event that  $C_d = 1$  for some  $d \in Q_n$ ,

$$\mathbf{P}[F_n] \geq \mathbf{P}[F_n \mid \exists C_d = 1, d \in Q_n] \mathbf{P}[\exists C_d = 1, d \in Q_n].$$

By Lemma 14 we have that  $\mathbf{P}[\exists C_d = 1, d \in Q_n] = 1 - o(1)$ , so it suffices to show that

$$\mathbf{P}[F_n \mid \exists C_d = 1, d \in Q_n] = 1 - o(1).$$

Fix  $d \in Q_n$  with  $C_d = 1$ , we will prove

$$\mathbf{P}[d^2 \mid \Phi(\pi)] = o(1).$$

From our construction of  $Q_n$ , there exists a prime  $p > n^{\lambda\beta}$  such that

$$\{d^2 \mid \Phi(\pi)\} \subset \{p \mid \frac{\Phi(\pi)}{d}\}.$$

For such prime number  $p$ , the event on the right hand side above satisfies

$$\{p \mid \frac{\Phi(\pi)}{d}\} \subset \left\{ \sum_{i=1}^{n/p} C_{ip} > 1 \right\}$$

Call the last event  $G_n$ . The Feller coupling at (8) allows us to bound the probability by

$$(32) \quad \mathbf{P}[G_n] \leq \mathbf{P}\left[\sum_{i=1}^{\lceil n/d \rceil} Y_{ip} + \mathbf{1}\{J_n = ip\} > 1\right].$$

This, in turn, is bounded by

$$\mathbf{P}\left[\text{Poi}\left(\sum_{i=1}^{\lceil n/p \rceil} \frac{\alpha}{ip}\right) > 0\right] + \mathbf{P}\left[\sum_{i=1}^{\lceil n/p \rceil} \mathbf{1}\{J_n = ip\} > 0\right].$$

The mean of the above Poisson random variable is asymptotically bounded by  $\alpha \log(n/p)/p$ , which is  $o(1)$  since  $p \geq n^{\lambda\beta}$ . This ensures that the left summand is  $o(1)$ . To bound the right summand we write

$$\mathbf{P}\left[\sum_{i=1}^{\lfloor n/p \rfloor} \mathbf{1}\{J_n = ip\} > 0\right] \leq \sum_{ip \leq n-n^\gamma} \mathbf{P}[J_n = ip] + \sum_{ip > n-n^\gamma} \mathbf{P}[J_n = ip].$$

We begin by bounding the first summand of the right hand side. By Lemma 10 (9),

$$\begin{aligned} \sum_{ip \leq n-n^\gamma} \mathbf{P}[J_n = ip] &\leq \sum_{i=1}^{\lfloor (n-n^\gamma)/p \rfloor} \frac{\alpha}{n-ip} \\ &\leq \int_1^{\frac{n-n^\gamma}{p}+1} \frac{\alpha}{n-px} dx \\ &= O\left(\frac{\log n}{p}\right) \\ &= o(1). \end{aligned}$$

The last line follows since  $p \geq n^{\lambda\beta}$ . For the second summand, from Lemma 10 (10) there exists some constant  $c > 0$  such that

$$\begin{aligned} \sum_{ip > n-n^\gamma} \mathbf{P}[J_n = ip] &\leq \sum_{ip > n-n^\gamma} cn^{-\alpha(1-\gamma)} \\ &\leq cn^{\gamma-\lambda\beta} n^{-\alpha(1-\gamma)}. \end{aligned}$$

The last line follows as there are at most  $n^{\gamma-\lambda\beta}$  different values of  $i$  such that  $n-n^\gamma < ip \leq n$ .

We therefore have that

$$\mathbf{P}[G_n] = O\left(n^{\gamma-\lambda\beta-\alpha(1-\gamma)}\right).$$

An easy calculation confirms that  $\gamma$  satisfying

$$\gamma < \frac{\alpha + \lambda\beta}{1 + \alpha}$$

is sufficient to ensure

$$\mathbf{P}[G_n] = o(1).$$

Choosing a suitable  $\gamma$ , it follows that

$$\mathbf{P}[F_n] = 1 - o(1),$$

completing our proof.  $\square$

*Proof of Theorem 4.* By Lemma 15 with probability  $1 - o(1)$  there exists a cycle length of length  $d$  satisfying (29) and (30). When these conditions are met, for  $K = \Phi(\pi)/d$ , we have  $\pi^K$  displaces  $d \leq n^\beta$  elements. Thus, with high probability  $\pi$  has minimal degree no more than  $n^\beta$ . This completes our proof.  $\square$

*Proof of Theorem 5.* The theorem statement is such that if it holds for  $\omega(n)$ , then it also holds for any  $\omega'(n) \geq \omega(n)$ . So, it suffices to prove the statement for all  $\omega(n) \leq \sqrt[4]{\log n}$ .

Fix such an  $\omega(n)$  and set  $b_n = n \exp(-\omega(n)\sqrt{\log n})$ . Let  $P$  be the set of all primes and define  $P_n = P \cap [b_n, n]$ . Given  $p \in P_n$  let  $I_p = [1, 2, \dots, \lfloor n/p \rfloor]$  be the set of all  $i$  for which  $pi$

is a multiple of  $p$  between  $p$  and  $n$ . We also introduce the entire collection of such multiples smaller than  $n$

$$W_n = \bigcup_{p \in P_n} \{(p, i) : i \in I_p\}.$$

It suffices to show that the event

$$E_n = \{\exists (p, i) \in W_n : ip \mid \Phi(\pi)\}$$

occurs with high probability. We can write  $E_n$  as a union of events,

$$E_n = \bigcup_{(p, i) \in W_n} \{C_{ip}^{(n)} > 0\}.$$

Notice that any two numbers in the set of products

$$\{ip : (p, i) \in W_n\}$$

are different. To see this we argue by contradiction, suppose that  $ip = i'p'$  with  $p < p'$ . Because of primality, this could only happen if  $p' \mid i$ . Thus  $i \geq p'$ . Also note that our assumption  $\omega(n) \leq \sqrt[4]{\log n}$  ensures  $b_n > \sqrt{n}$ . Thus,  $p, p' > \sqrt{n}$ . These two inequalities give

$$ip \geq p'p > \sqrt{n}\sqrt{n} = n.$$

But  $ip > n$  is a contradiction, since our construction of  $I_p$  ensures that  $ip \leq n$ .

We have now shown that the occurrence of  $E_n$  is equivalent to the sum of cycle counts being positive:  $E_n = \{\sum_{W_n} C_{ip} > 0\}$ . The Feller coupling (8) ensures that

$$(33) \quad \sum_{W_n} C_{ip} \geq -D_n + \sum_{W_n} Y_{ip},$$

with  $D_n$  the total number of deletions. It follows that

$$(34) \quad \mathbf{P}[E_n] \geq \mathbf{P}[-D_n + \sum_{W_n} Y_{ip} > 0].$$

Using additivity of independent Poisson random variables, the sum on the right of (33) is distributed as a Poisson with mean

$$(35) \quad \begin{aligned} \mu_{n, \alpha} &= \sum_{p \in P_n} \sum_{i=1}^{\lfloor n/(p) \rfloor} \alpha/ip \approx \alpha \sum_{p \in P_n} \frac{\log(n/(p))}{p} \\ &= \alpha \left( \log n \sum_{p \in P_n} \frac{1}{p} - \sum_{p \in P_n} \frac{\log p}{p} \right). \end{aligned}$$

Lemma 16 shows that  $\mu_{n, \alpha} \rightarrow \infty$ . To establish that (34) occurs with high probability, we will show that the number of deletions,  $D_n$ , in the Feller coupling is unlikely to remove every successful  $Y_{ip}$  in (33).

As  $\mu_{n, \alpha} \rightarrow \infty$ , we take any  $h(n) = o(\mu_{n, \alpha})$  with  $h(n) \rightarrow \infty$ . By Lemma 10 (12) we know that  $\mathbf{E}D_n \leq c$  for some  $c = c(\alpha)$ . It follows from Markov's inequality that

$$\mathbf{P}[D_n \geq h(n)] \leq \frac{c}{h(n)} = o(1).$$

Standard estimates on a Poisson random variable tell us that

$$\mathbf{P}[\text{Poi}(\mu_{n, \alpha}) \leq h(n)] = 1 - o(1).$$

So  $D_n$  is with high probability smaller than  $\sum_{W_n} Y_{ip}$ , and combined with (33) we have established that the right side of (34) occurs with high probability.  $\square$

**Lemma 16.** *Let  $\mu_{n,\alpha}$  be as in the proof of Theorem 5. It holds that  $\mu_{n,\alpha} \rightarrow \infty$ .*

*Proof.* It suffices to show that (35) tends to infinity. Two classical theorems attributed to Euler ([Eul37]) and Chebyshev ([Apo76]), respectively, state that for sums of primes smaller than  $n$

$$\sum_{p \leq n} \frac{1}{p} = \log \log n + O(1) \quad \text{and} \quad \sum_{p \leq n} \frac{\log p}{p} = \log n + O(1).$$

Recalling that  $P_n = P \cap [b_n, n]$ , it follows that (35) is asymptotic to

$$\log n \log \frac{\log n}{\log b_n} - \log \frac{n}{b_n}.$$

We can express the second term precisely

$$(36) \quad \log \frac{n}{b_n} = \log \exp \left( \omega(n) \sqrt{\log n} \right) = \omega(n) \sqrt{\log n}.$$

Similarly we compute the order of the first term. Notice

$$(37) \quad \begin{aligned} \log \frac{\log n}{\log b_n} &= \log \left( \frac{\log n}{\log n - \omega(n) \sqrt{\log n}} \right) \\ &= \log \left( 1 + \frac{\omega(n) \sqrt{\log n}}{\log n - \omega(n) \sqrt{\log n}} \right). \end{aligned}$$

As  $\omega(n) \leq \sqrt[4]{\log n}$  the above term is  $\log(1 - o(1))$ . Using the fact that  $\log(1 - x) \approx -x$  as  $x \rightarrow 0$  we have (37) is asymptotic to

$$\frac{\omega(n) \sqrt{\log n}}{\log n - \omega(n) \sqrt{\log n}}.$$

Reintroducing the  $\log n$  factor, we now have

$$(38) \quad \log n \sum_{P_n} \frac{1}{p} \approx \log n \frac{\omega(n) \sqrt{\log n}}{\log n - \omega(n) \sqrt{\log n}}.$$

Combining (36) and (38) gives

$$\begin{aligned} \mu_{n,\alpha} &\approx \log n \frac{\omega(n) \sqrt{\log n}}{\log n - \omega(n) \sqrt{\log n}} - \omega(n) \sqrt{\log n} \\ &= \omega(n)^2 \frac{\log n}{\log n - \omega(n) \sqrt{\log n}} \\ &= \omega(n)^2 (1 - o(1)) \end{aligned}$$

Since  $\omega(n) \rightarrow \infty$  we conclude that  $\mu_{n,\alpha} \rightarrow \infty$ . □

Now we set our sights on proving Theorem 3. This will require Theorem 4 and Theorem 5, as well as a few additional lemmas.

**Lemma 17.** *Let  $0 < \gamma < 1$  and  $\psi(n) \rightarrow \infty$  such that  $\psi(n) = o(\log n)$ . The probability that simultaneously for all  $2 \leq r \leq \exp(\psi(n))$  there exists  $C_{j_r} > 0$  such that  $j_r > n^\gamma$  and  $r \nmid j_r$  is  $1 - o(1)$ .*

*Proof.* Let  $r_0 = \exp(\psi(n))$  and consider the complement of the event in question:

$$E = \{\exists r < r_0 : r \mid j \text{ for all } n^\gamma < j \text{ such that } C_j > 0\}.$$

It suffices to show that  $\mathbf{P}[E] = o(1)$ . In order to model the values  $C_j$  with independent Poisson random variables we will work with a larger event. For any  $\gamma < \gamma' < 1$ , we consider

$$E_{\gamma'} = \{\exists r < r_0 : r \mid j \text{ for all } n^\gamma < j < n^{\gamma'} \text{ such that } C_j > 0\}.$$

A union bound leads to

$$\begin{aligned} \mathbf{P}[E_{\gamma'}] &\leq \sum_{r=2}^{r_0} \mathbf{P}[r \mid j \text{ for all } n^\gamma < j < n^{\gamma'} \text{ such that } C_j > 0] \\ (39) \quad &= \sum_{r=2}^{r_0} \mathbf{P}[C_j = 0 \text{ for all } n^\gamma < j < n^{\gamma'} \text{ such that } r \nmid j]. \end{aligned}$$

Let  $A_r$  be the set of integers in  $(n^\gamma, n^{\gamma'})$  that  $r$  fails to divide. Formally,

$$A_r = [n^\gamma, n^{\gamma'}] \cap ([n] \setminus \{ir : i \leq \lfloor n/r \rfloor\}).$$

As  $n^{\gamma'} = o(n)$  we can apply [ABT00, Theorem 3.1] to conclude that  $C[n^\gamma, n^{\gamma'}] \xrightarrow{TV} Y[n^\gamma, n^{\gamma'}]$ . Thus, the probabilities at (39) converge to

$$(40) \quad \sum_{r=2}^{r_0} \prod_{j \in A_r} \mathbf{P}[Y_j = 0] = \sum_{r=2}^{r_0} \exp\left(-\sum_{j \in A_r} \frac{\alpha}{j}\right).$$

The quantity  $\sum_{j \in A_r} \frac{\alpha}{j}$  is minimized at  $r = 2$ , and in this case  $\sum_{j \in A_2} \frac{1}{j} \gg \log n$ . We can apply this to (40) to obtain

$$\mathbf{P}[E_{\gamma'}] \leq \sum_{r=2}^{r_0} n^{-\delta} \leq r_0 n^{-\delta} = o(1),$$

for some  $\delta > 0$ . As  $E \subseteq E_{\gamma'}$ , this completes the proof.  $\square$

**Lemma 18.** *Let  $\delta = \delta(\varepsilon, \alpha) = 1 - (\alpha + \varepsilon) \log 2$ . For any  $\varepsilon > 0$ , there exists a constant  $c = c(\varepsilon, \alpha)$  such that the probability of  $\pi$  fixing a set of size  $k$  is bounded by  $ck^{-\delta}$  uniformly for all  $1 \leq k \leq n/2$ .*

*Proof.* In Lemma 22 we show that  $\mathbf{P}[k \in \mathcal{L}(\mathbf{X}(\alpha))] \leq Ck^{-\delta}$  for some  $C$  and all  $k \leq n$ . The Feller coupling lets us relate the probability of a fixing a set size to this quantity, the only complication is a possible contribution from  $\mathbf{1}\{J_n = \ell\}$ . However, the location of this extra cycle is unconcentrated enough to not alter the order of these probabilities.

Lemma 10 (9) ensures that  $\mathbf{P}[J_n = \ell] \leq \frac{\alpha}{n-\ell}$ . We make use of this as we condition on the value of  $J_n$ .

$$(41) \quad \mathbf{P}[\pi \text{ has a } k\text{-cycle}] \leq \mathbf{P}[k \in \mathcal{L}(\mathbf{X}(\alpha))] + \sum_{\ell \leq k} \mathbf{P}[k - \ell \in \mathcal{L}(\mathbf{X}(\alpha))] \mathbf{P}[J_n = \ell]$$

$$(42) \quad \leq Ck^{-\delta} + \sum_{\ell \leq k} C(k - \ell)^{-\delta} \frac{\alpha}{n - \ell}$$

$$\begin{aligned} (43) \quad &\leq Ck^{-\delta} + \frac{2\alpha}{n} \sum_{\ell \leq k} C\ell^{-\delta} \\ &\leq Ck^{-\delta} + C'n^{-\delta}. \end{aligned}$$

Where at (42) we use our bound on  $\mathbf{P}[k \in \mathcal{L}(\mathbf{X}(\alpha))]$  from Lemma 22 and bound  $\mathbf{P}[J_n = \ell]$  with Lemma 10 (9). The next line, (43), reindexes the sum and uses that  $\ell \leq n/2$  to bound  $\frac{\alpha}{n-\ell} \leq 2\alpha/n$ . Our claim then follows by bounding the leftmost sum by  $n^{-\delta}$  time some constant  $C'$ , and the fact that  $k^{-\delta} > n^{-\delta}$ .  $\square$

We now prove a result analogous to [LP93, Theorem 1]. Namely, that if a permutation sampled according to Ewen's sampling formula is in a transitive subgroup, this subgroup is likely to be either all of  $S_n$  or the alternating group,  $A_n$ . Though the lemmas culminating to this used rather different arguments, our proof from here closely follows that in [LP93]. Recall that a *primitive subgroup* is a transitive subgroup that does not fix any partition of  $[n]$ .

*Proof of Theorem 3.* Let  $\pi \in G$  for a transitive subgroup  $G$ . According to [GM98], it follows from results of [Bab81] that the minimal degree of a primitive subgroup not containing  $A_n$  is at least  $(\sqrt{n} - 1)/2$ . On the other hand, by Theorem 4 with high probability the minimal degree of  $\langle \pi \rangle$  is less than  $n^{0.4}$ . Thus, the probability that  $G$  is primitive is  $o(1)$ .

Assume  $G$  is a non-primitive, transitive subgroup. Then it must fix some partition  $\{B_i\}_{i=1}^r$  of  $[n]$ . By transitivity every block in such a partition will be mapped to every other, thus the partition must be into blocks of equal size, that is

$$|B_i| = \frac{n}{r}.$$

Note that any cycle of a permutation that preserves this partition must have the same number of elements in each block it acts on. We will use this to establish that any  $\pi \in G$  with high probability cannot fix this partition for any  $r$ .

We consider three cases for the possibly amount,  $r$ , of blocks:

**Case 1:**  $2 \leq r \leq r_0 = \exp(\log \log n \sqrt{\log n})$

By Lemma 17 with  $\psi(n) = \log \log n \sqrt{\log n}$ , with high probability for every  $r$  there exists there exists  $j_r > n^{.99}$  such that  $\pi$  contains a cycle of length  $j_r$  and  $r \nmid j_r$ . Fix some  $r$  and  $j_r$ , and let  $B$  be the union of all blocks this cycle acts upon. Because  $r$  does not divide  $j_r$ ,  $B$  is a proper invariant subset of  $[n]$  with size  $sn/r$ , where  $s$  is the number of blocks in  $B$ . By Lemma 18 this occurs with probability bounded by

$$\sum_{r=2}^{r_0} \sum_{s=1}^r c(sn/r)^{-\delta} \leq cr_0^2(n/r_0)^{-\delta} = o(1).$$

**Case 2:**  $r_0 \leq r \leq n/r_0$

By Theorem 5, with high probability there exists a prime  $q > n/r_0$  that divides  $\Omega(\pi)$ . Thus there exists a cycle of length  $j$  such that  $q \mid j$ . Let  $t \leq r$  be the number of blocks this cycle intersects. Because of the bounds on  $r$  we have

$$\frac{j}{t} \leq |B_i| = \frac{n}{r} \leq \frac{n}{r_0} < q.$$

Since  $q$  divides  $j = t \frac{j}{t}$  and  $\frac{j}{t} < q$  by the above inequality, we must have that  $q \mid t$ . However, the total number of blocks  $r$  satisfies

$$r < \frac{n}{r_0} < q$$

so this is impossible.

**Case 3:**  $n/r_0 \leq r < n$

Let  $a$  be as in Proposition 13 and  $\varepsilon > 0$  such that  $a + \varepsilon < 1$ . Using Lemma 17 with  $\psi(n) = \log \log n \sqrt{\log n}$  one more time, we now find  $j > n^{a+\varepsilon}$  such that  $\pi$  contains a cycle of length  $j$  and the blocks size,  $s = n/r$  does not divide  $j$ . Again, let  $B$  be the union of blocks which intersect this cycle. Because the size of the blocks does not divide  $j$ , this intersection is a proper subset of  $B$ . We conclude that  $\pi$  must contain another cycle of length  $j'$  that intersects each block in  $B$ . Hence both cycle lengths  $j$  and  $j'$  are divisible by the number of blocks in  $B$ . We bound the number of blocks,

$$\frac{|B|}{s} > \frac{j}{s} > \frac{n^{a+\varepsilon}}{s} > n^a.$$

However, by Proposition 13 with probability  $1 - o(1)$  no two cycle lengths have a common divisor greater than  $n^a$ . This completes our proof.  $\square$

**3.3. Proving Proposition 7.** To rule out generating  $A_n$  we need an estimate that shows an  $ESF(\alpha, n)$  permutation is odd with probability bounded away from zero. Of course this probability ought to converge to  $1/2$ , but we were unable to find a proof. We make due with an absolute lower bound.

**Lemma 19.** *Let  $\pi \sim ESF(\alpha, n)$ , then*

$$\inf_{n \geq 2} \min\{\mathbf{P}[\pi \text{ is odd}], \mathbf{P}[\pi \text{ is even}]\} \geq \min\left\{\frac{1}{\alpha+1}, \frac{\alpha}{\alpha+1}\right\}.$$

*Proof.* We will proceed by induction. It is straightforward to check via the Feller coupling that an  $ESF(\alpha, 2)$  permutation is odd with probability  $\frac{\alpha}{\alpha+1}$ , and it is even with probability  $1 - \frac{\alpha}{\alpha+1} = \frac{1}{\alpha+1}$ .

Suppose that for  $2 \leq m \leq n-1$ , if  $\pi_m \sim ESF(\alpha, m)$  then

$$\min\{\mathbf{P}[\pi_m \text{ is odd}], \mathbf{P}[\pi_m \text{ is even}]\} \geq \varepsilon,$$

for some yet to be determined  $\varepsilon > 0$ . Now, it suffices to prove that

$$(44) \quad \min\{\mathbf{P}[\pi \text{ is odd}], \mathbf{P}[\pi \text{ is even}]\} \geq \varepsilon.$$

Consider the sequence  $\xi_1, \xi_2, \dots$  of Bernoulli random variables for the Feller coupling. Recall that  $J_n = (n+1) - R_n$ , with  $R_n$  the index of the rightmost 1 in  $\xi_1, \dots, \xi_n$ . We will condition on the value of  $J_n$ , but need to also take into account the parity of  $n$ .

**$n$  is odd:** We condition on the value of  $J_n$ . For convenience let  $q_\ell = \mathbf{P}[J_n = \ell]$ . If  $J_n = \ell$ , then  $\xi_{n+1-\ell} = 1$  and we can view the beginning sequence  $\xi_1, \dots, \xi_{n-\ell}, 1$  as corresponding to a random permutation sampled with distribution  $ESF(\alpha, n-\ell)$ . We denote such a permutation by  $\pi_{n-\ell}$ . Noting that when  $J_n = n$ ,  $\pi$  is a single  $n$ -cycle and therefore even, it follows that

$$\mathbf{P}[\pi \text{ is odd}] = \sum_{\ell \text{ odd}}^{n-3} \mathbf{P}[\pi_{n-\ell} \text{ is even}] q_\ell + \sum_{\ell \text{ even}}^{n-2} \mathbf{P}[\pi_{n-\ell} \text{ is odd}] q_\ell + q_{n-1}.$$

By the inductive hypothesis

$$\mathbf{P}[\pi \text{ is odd}] \geq \sum_{\ell=1}^{n-2} \varepsilon q_\ell + q_{n-1}.$$



Since  $\sum_1^n q_\ell = \sum_1^n \mathbf{P}[J_n = \ell] = 1$ , it suffices to prove that  $q_{n-1} \geq \varepsilon(q_{n-1} + q_n)$ . Equivalently, this requires that  $(1 - \varepsilon)q_{n-1} \geq \varepsilon q_n$ . Notice that

$$q_{n-1} = \mathbf{P}[\xi_2 = 1] \prod_{i=3}^n \mathbf{P}[\xi_i = 0], \text{ and } q_n = \prod_{i=2}^n \mathbf{P}[\xi_i = 0].$$

Much of this cancels when we solve  $(1 - \varepsilon)q_{n-1} \geq \varepsilon q_n$ , so we arrive at the requirement

$$(1 - \varepsilon) \frac{\mathbf{P}[\xi_2 = 1]}{\mathbf{P}[\xi_2 = 0]} \geq \varepsilon.$$

The ratio  $\frac{\mathbf{P}[\xi_2=1]}{\mathbf{P}[\xi_2=0]} = \alpha$ , and thus we require

$$(45) \quad (1 - \varepsilon)\alpha \geq \varepsilon.$$

*n even:* The argument is similar. The key difference is that we instead need  $q_n \geq \varepsilon(q_{n-1} + q_n)$ .

Rewriting as before this is the same as

$$(46) \quad \varepsilon\alpha \leq (1 - \varepsilon).$$

After solving for  $\varepsilon$  in (45) and (46), we see that (44) holds whenever  $0 < \varepsilon \leq \min \left\{ \frac{1}{\alpha+1}, \frac{\alpha}{\alpha+1} \right\}$ .  $\square$

*Remark 20.* When  $\alpha = 1$  this confirms the intuition that even and odd permutations occur with probability  $1/2$  for all  $n \geq 2$ .

**Corollary 21.** *Let  $\delta = \delta(\alpha, \varepsilon)$  and  $c = c(\alpha, \varepsilon)$  be as in Lemma 18. It holds for all  $k \leq n/2$  that*

$$\mathbf{P}[\pi \text{ fixes a } k\text{-set} \mid \pi \text{ is odd}] \leq ck^{-\delta} \cdot \max \left\{ \frac{\alpha+1}{\alpha}, \frac{\alpha+1}{1} \right\}.$$

*Proof.* We start with the reformulation

$$\mathbf{P}[\pi \text{ fixes a } k\text{-set} \mid \pi \text{ is odd}] = \frac{\mathbf{P}[\pi \text{ fixes a } k\text{-set and } \pi \text{ is odd}]}{\mathbf{P}[\pi \text{ is odd}]}.$$

The numerator is bounded by  $\mathbf{P}[\pi \text{ fixes a } k\text{-set}]$  which is less than  $ck^{-\delta}$  by Lemma 18. We bound the denominator away from zero by Lemma 19, completing our proof.  $\square$

#### 4. THE UPPER BOUND FOR $s_\alpha$

We carry out the plan described in Section 1.4. First we bound the quenched probability  $\tilde{p}_k$  defined formally just below here. The proof is similar to [PPR15, Lemma 3.1]. We repeat a selection of the details for clarity, and point out where the argument differs with general  $\alpha$ . Subsequently, we mirror [PPR15, Theorem 3.2] as we apply the Borel Cantelli lemma.

Recall the functions  $f_k$  and  $g_k$  from (5). Namely that  $f_k$  is the number of available summands smaller than  $k$ , and  $g_k$  is the largest sum attainable with them. Also, define

$$\begin{aligned} \tau_\varepsilon &:= \sup\{k : f_k \geq (\alpha + \varepsilon) \log k\}, \\ \tau &:= \sup\{n : g_{\lambda_k} \geq k\}, \end{aligned}$$

where  $\varepsilon > 0$  is yet to be chosen, but small, and  $\lambda_k := \left\lfloor \frac{k}{\alpha \log k} \right\rfloor$ . The proofs of [PPR15, Lemma 2.1, Lemma 2.2] generalize in a straightforward way, so that  $T = T(\varepsilon, \delta) := \max\{\tau_\varepsilon, \tau\}$  is almost surely finite. As  $\mathbf{P}[T > \lambda_k] \rightarrow 0$ , we define the quenched probabilities to avoid this diminishing sequence of events

$$\tilde{p}_k := \mathbf{P}[T < \lambda_k \text{ and } k \in \mathcal{L}(\mathbf{X})].$$

**Lemma 22.** *Suppose that  $\alpha < 1/\log 2$ . For each  $\varepsilon > 0$  there exists  $C = C(\varepsilon)$  such that for all  $k \geq 1$ ,*

$$\tilde{p}_k(\alpha) \leq Ck^{-1+(\alpha+\varepsilon)\log 2}.$$

*Proof.* Fix  $\varepsilon > 0$ . Let  $G_k$  be the event that  $T < \lambda_k$  while also  $n \in \mathcal{L}(\mathbf{X})$ . Call a sequence  $\mathbf{y} = (y_1, y_2, \dots)$  admissible if it is coordinate-wise less than or equal to  $\mathbf{X}$ . When  $G_k$  occurs, it is not possible for  $n$  to be a sum of  $\sum_j jy_j$  for an admissible  $\mathbf{y}$  with  $y_j$  vanishing for  $j > \lambda_k$ . Indeed, on the event  $G_k$ , we have  $\sum_{j \leq \lambda_k} jX_j < n$ . The event satisfying the following three conditions contains  $G_k$ :

- (i)  $f_{\lambda_k} \leq (\alpha + \varepsilon) \log \lambda_k$ .
- (ii)  $g_{\lambda_k} < n$ .
- (iii) There is some  $k$  with  $k = \sum_j (y'_j + y''_j)$  with  $\mathbf{y}'$  supported on  $[0, \lambda_k]$  and  $\mathbf{y}''$  nonzero and supported on  $[\lambda_k + 1, k]$  with both  $\mathbf{y}'$  and  $\mathbf{y}''$  admissible.

Define the probability  $p'_k = \mathbf{P}[f_{\lambda_k} \leq (\alpha + \varepsilon) \log \lambda_k \text{ and } g_{\lambda_k} < n \text{ and } \ell = \sum_j jy'_j]$  where  $\mathbf{y}'$  is admissible and supported on  $[1, \lambda_n]$ . Also, define  $p''_\ell = \mathbf{P}[\ell = \sum_j jy''_j]$  where  $\mathbf{y}''$  is admissible and supported on  $[\lambda_k + 1, k]$ . Using independence we can obtain an upper bound on  $\tilde{p}_k$  by decomposing into these two admissible vectors:

$$\begin{aligned} \tilde{p}_k &\leq \sum_{k=\lambda_k+1}^k p'_{k-\ell} p''_\ell \\ (47) \quad &\leq \left( \sum_{\ell=\lambda_k+1}^k p'_{k-\ell} \right) \max_{\lambda_k \leq \ell \leq k} p''_\ell. \end{aligned}$$

The first factor above is (by Fubini's theorem) equal to  $\mathbf{E}[\mathcal{L}(\mathbf{X}) \cap [0, \lambda_k]]$ . Using the trivial bound where we assume each sum from  $\mathbf{X}$  is distinct, and that we are working on the event  $f_{\lambda_k} \leq (\alpha + \varepsilon) \log \lambda_k$  we have

$$(48) \quad |\mathcal{L}(\mathbf{X}) \cap [0, \lambda_k]| \leq 2^{Z_m} \leq \lambda_k^{(\alpha+\varepsilon)\log 2}.$$

We now bound the second term. We will show there exists a constant  $C$  such that

$$(49) \quad p''_\ell \leq C \frac{\log^2 k}{k}, \text{ for all } \ell \in [\lambda_k + 1, k].$$

Let  $H$  be the event that  $X_j \geq 2$  for some  $j \in [\lambda_k, k]$ . As  $\mathbf{P}[X_j \geq 2] \leq \alpha/j^2$  we can write

$$(50) \quad \mathbf{P}[H] \leq \sum_{j=\lambda_k}^k \alpha/j^2 \leq \alpha/\lambda_k \ll \frac{\log k}{k}.$$

The event that  $\ell = \sum_j jy''_j$  for an admissible  $\ell$  supported on  $[\lambda_k, k]$ , but that  $H$  does not occur is contained in the union of events  $E_j$  that  $X_j = 1$  and  $\ell = j = \sum_i iy''_i$  for some admissible  $\mathbf{y}''$  supported on  $[\lambda_k, k] \setminus \{j\}$ . Using independence of  $X_j$  from the other coordinates of  $\mathbf{X}$ ,

along with our description of what must happen if  $H$  does not, we obtain

$$\begin{aligned}
 p''_\ell &\leq \mathbf{P}[H] + \sum_{j=\lambda_k}^k \frac{1}{j} p''_{\ell-j} \\
 &\leq \mathbf{P}[H] + \frac{1}{\lambda_k} \sum_{j=\lambda_k}^k p''_{\ell-j} \\
 (51) \quad &\leq \frac{\log k}{k} \left( 1 + \sum_{j=\lambda_k}^k p''_{\ell-j} \right).
 \end{aligned}$$

It remains to bound the summation in the last factor. Here taking  $\alpha \neq 1$  is a minor nuisance, but we circumvent any difficulties with the crude bound  $\alpha \leq 2$ . The idea is to use the generating function

$$F(z, \mathbf{X}) := \prod_{j \in [\lambda_k, k]: X_j=1} (1 + z^j).$$

Writing  $[z^j]F$  for the  $j$ th coefficient of  $F$ . Observe that this corresponds to forming  $j$  using the  $j \in [\lambda_k, k]$  for which  $X_j = 1$ . It follows that

$$\sum_{j=\lambda_k}^k p''_{\ell-j} \leq \sum_{j=\lambda_k}^k \mathbf{E}([z^{\ell-j}]F(z, \mathbf{X})).$$

Using that  $[z^j]F(z, \mathbf{X}) \leq F(1, \mathbf{X})$  we can bound the above line by  $\mathbf{E}F(1, \mathbf{X})$ . This is tractable using independence of the  $X_j$ . Carrying the calculation out we obtain

$$\begin{aligned}
 \mathbf{E}F(1, \mathbf{X}) &= \prod_{j=\lambda_k}^n \mathbf{E}[1 + \mathbf{1}\{X_j = 1\}] \\
 &= \prod_{j=\lambda_k}^k \left( 1 + \frac{\alpha}{j} \right) \\
 &\leq \prod_{j=\lambda_k}^n \left( 1 + \frac{2}{j} \right).
 \end{aligned}$$

The last term can be expanded and written as

$$\frac{k^2 + 3k + 2}{\lambda_k^2 + \lambda_k} \ll \frac{k^2}{\lambda_k^2} \ll \log^2 k.$$

Combine this with (51) and we have

$$p''_\ell \ll \frac{\log k}{k} (1 + \log^2 k) \ll \frac{\log^3 k}{k}.$$

This yields (49). To conclude we plug (48) and (49) into (47) and arrive at

$$\tilde{p}_k \leq C(k - \lambda_k)^{(\alpha+\varepsilon) \log 2} \frac{\log^3 k}{k}.$$

This is bounded above by a constant multiple of  $k^{-1+(\alpha+2\varepsilon) \log 2}$ , which, after swapping all  $\varepsilon$ 's for  $\varepsilon/2$ , establishes the lemma. □

**Proposition 23.** *Let  $s_\alpha$  be as in Theorem 6 and  $h(\alpha)$  be as in (4). For continuity points of  $h$  it holds that  $s_\alpha \leq h(\alpha)$ , and  $s_\alpha \leq h(\alpha) + 1$  for all  $\alpha$ .*

*Proof of Proposition 23.* Fix a small  $\varepsilon > 0$  and let  $s_{\alpha,\varepsilon} = \lceil (1 - (\alpha - 2\varepsilon) \log 2)^{-1} \rceil$ . Sample  $s_{\alpha,\varepsilon}$  vectors  $\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(s_{\alpha,\varepsilon})}$  and let  $T(\mathbf{X}^{(1)}), \dots, T(\mathbf{X}^{(s_{\alpha,\varepsilon})})$  be the a.s. random times distributed as  $T$ . Take  $T^* = \max\{T(\mathbf{X}^{(i)})\}_1^{s_{\alpha,\varepsilon}}$ . By independence of the  $\mathbf{X}^{(i)}$  and the bound in Lemma 22 we have the probability that  $T^* < \lambda_k$  and  $k \in \mathcal{L}(\mathbf{X}^{(i)})$  for all  $1 \leq i \leq s_{\alpha,\varepsilon}$  is at most a constant multiple of  $k^{s_{\alpha,\varepsilon}(-1+(\alpha+\varepsilon)\log 2)}$ . Our choice of  $s_{\alpha,\varepsilon}$  ensures that the exponent is less than  $-1$ . The series is thus summable. It follows that finitely many  $k > T^*$  belong to the intersection of the  $\mathcal{L}(\mathbf{X}^{(i)})$ . As  $T^*$  is almost surely finite (the proof of this can be found in [PPR15, Section 2]), the result follows by letting  $\varepsilon \rightarrow 0$  so that  $s_{\alpha,\varepsilon} \rightarrow h(\alpha)$ .  $\square$

## 5. THE LOWER BOUND FOR $s_\alpha$

Here we establish the lower bounds on  $m_\alpha$ .

**Proposition 24.** *Let  $s_\alpha$  be as in Theorem 6 and  $h(\alpha)$  be as in (4). For  $0 \leq \alpha < 1/\log 2$ , it holds that  $s_\alpha \geq h(\alpha)$ . When  $\alpha \geq 1/\log 2$  it holds that  $s_\alpha = \infty$ .*

We prove this by a Fourier-analytic argument. We begin by considering continuity points  $\alpha$  of  $h$ , and set  $m = h(\alpha)$ . We then fix  $m$  i.i.d. Poisson vectors  $\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}$ .

**Lemma 25.** *Let  $I = (0, k]$  and let  $\varepsilon > 0$ . Then the event*

$$A = \left\{ \bigcup_{i=1}^m \mathcal{L}(I, \mathbf{X}^{(i)}) \subset \left[0, \frac{mk}{\alpha\varepsilon}\right] \right\}$$

*holds with probability  $\mathbf{P}[A] \geq 1 - \varepsilon$ .*

*Proof.* This is a straightforward application of Markov's inequality.  $\square$

Recall our notation that  $\mathbf{X}^{(i)} = (X_j^{(i)})_{j=1}^\infty$ .

**Lemma 26.** *Fix  $\varepsilon \in (0, 1/2)$ . For any  $\delta > 0$ , there is a constant  $C = C(\varepsilon, \delta, m, \alpha)$  such that the event*

$$(52) \quad E = E(\varepsilon, \delta, m, \alpha) := \left\{ \min_i \sum_{\ell < j \leq k} X_j^{(i)} \geq (1 - \delta)\alpha \log(k/\ell) - C \quad \forall 1 \leq \ell \leq k \right\}$$

*holds with probability  $\mathbf{P}[E] \geq 1 - \varepsilon$ .*

We remark that this is a straightforward generalization of [EFG15a, Lemma 3.3].

*Proof.* In fact, we will take  $C \gg \frac{1}{\alpha\delta^2} \log(m/\varepsilon)$  while ensuring that  $C \geq 1$ . Note that the claim holds vacuously when  $\ell \geq e^{-C}k$ , so we need only consider the case  $\ell < e^{-C}k$ .

Fix  $1 \leq i \leq m$  and let  $B$  denote the event that  $\sum_{\ell < j \leq k} X_j^{(i)} < (1 - \delta)\alpha \log(k/\ell) - 1$  for some  $\ell \leq e^{-C}k$ . Writing  $\ell'$  for the smallest power of 2 with  $\ell' > \ell$ , we thus have

$$(53) \quad \sum_{\ell' < j \leq k} X_j^{(i)} \leq \alpha(1 - \delta) \log(k/\ell')$$

on  $B$ .

Let  $\mathbb{D} = \{2^i\}_{i \geq 0}$  denote the set of non-negative powers of 2. From (53) it follows that

$$(54) \quad 1_B \leq \sum_{\substack{\ell' \leq 2e^{-C}k, \\ \ell' \in \mathbb{D}}} (1 - \delta) \sum_{\ell' < j \leq \ell} X_j^{(i)} - \alpha(1 - \delta) \log(k/\ell').$$

Each of the variables  $X_j^{(i)}$  are independent and Poisson with mean  $\mathbf{E}X_j^{(i)} = \frac{\alpha}{j}$ . For a Poisson variable  $P$  with mean  $\lambda$ , we have  $\mathbf{E}a^P = e^{\lambda(a-1)}$ . Moreover, the sum  $\sum_{\ell' < j \leq k} X_j^{(i)}$  is Poisson with mean  $\alpha \log(k/\ell') + O(1)$ . Taking expectations on both sides of (54) therefore yields

$$\mathbf{P}[B] \ll \sum_{\substack{\ell' \leq 2e^{-C}k, \\ \ell' \in \mathbb{D}}} \exp[-\alpha\delta - \alpha(1-\delta)\log(1-\delta)] \log(k/\ell')$$

Near zero,  $-\delta - (1-\delta)\log(1-\delta) = -(1+o(1))\delta^2$ . Therefore

$$\mathbf{P}[B] \ll \sum_{\substack{\ell' \leq 2e^{-C}k, \\ \ell' \in \mathbb{D}}} (k/\ell')^{-\alpha\delta^2} \ll e^{-\alpha\delta^2 C},$$

since the sum of the geometric series is bounded by a constant multiple of its first term. Choosing  $C \gg \frac{1}{\alpha\delta^2} \log(m/\varepsilon)$  ensures that  $\mathbf{P}[B] \leq \frac{\varepsilon}{m}$ , and now the claim follows by the union of events bound.  $\square$

An insight in [EFG15a] (to which they credit the idea to Maier and Tenenbaum from [MT84]) is that Fourier analysis may be used to obtain a lower bound on the size of the set

$$(55) \quad S(I; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}) := \left\{ (n_i - n_m)_{1 \leq i < m} : n_i \in \mathcal{L}(I, \mathbf{X}^{(i)}) \right\}.$$

We show that the technique extends to the present level of generality. Note that the analysis of [EFG15a] may be regarded as the special case  $m = 3$  and  $\alpha = 1$  of our arguments.

Let  $\mathbb{T} = \mathbb{R}/\mathbb{Z}$  be the unit torus. For  $\theta \in \mathbb{T}$ , let  $\|\theta\|$  denote the distance to  $\mathbb{Z}$  and set  $e(z) = e^{2\pi iz}$ . Write  $\boldsymbol{\theta} = (\theta_1, \dots, \theta_m) \in \mathbb{T}^m$ . Define

$$\mathbb{T}_0^m = \{\boldsymbol{\theta} \in \mathbb{T}^m : \theta_1 + \dots + \theta_m = 0\}.$$

Fix an interval  $I$ . We define the function  $F(\boldsymbol{\theta}) = F_I(\boldsymbol{\theta}, \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)})$  via the formula

$$(56) \quad F(\boldsymbol{\theta}) := \prod_{j \in I} \prod_{i=1}^m \left( \frac{1 + e(j\theta_i)}{2} \right)^{X_j^{(i)}}.$$

Writing  $\theta_m = -\theta_1 - \dots - \theta_{m-1}$ , we regard  $F(\boldsymbol{\theta})$  as a function on  $\mathbb{T}^{m-1}$ . It is straightforward to verify that its Fourier transform is a function  $\hat{F}: \mathbb{Z}^{m-1} \rightarrow \mathbb{C}$  supported on the set  $S(I; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)})$  defined above in (55).

The Cauchy-Schwarz inequality yields that

$$(57) \quad \sum_{a \in \mathbb{Z}^{m-1}} |\hat{F}(a)|^2 \sum_{a: \hat{F}(a) \neq 0} 1 \geq \left[ \sum_{a \in \mathbb{Z}^{m-1}} \hat{F}(a) \right]^2.$$

Recognizing that  $S(I; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}) \geq |\{a: \hat{F}(a) \neq 0\}|$ , that  $\sum_{a \in \mathbb{Z}^{m-1}} \hat{F}(a) = F(0) = 1$ , and that by Parseval's identity  $\sum_{a \in \mathbb{Z}^{m-1}} |\hat{F}(a)|^2 = \int_{\mathbb{T}_0^m} |F(\boldsymbol{\theta})|^2 d\boldsymbol{\theta}$ , it follows from (57) that

$$(58) \quad |S(I; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)})| \geq \left( \int_{\mathbb{T}_0^m} |F(\boldsymbol{\theta})|^2 d\boldsymbol{\theta} \right)^{-1}.$$

Our next task is to bound the integral appearing in (58). We will achieve this in two steps: first, by obtaining a pointwise bound with respect to  $\boldsymbol{\theta}$  in Lemma 27, and second, by integrating out the  $\boldsymbol{\theta}$  dependence in Corollary 28.

Let  $\beta \in (0, 1)$  be a real parameter satisfying

$$\beta \alpha \log 2 = 1 - m^{-1} + \delta_2,$$

where  $\delta_2 > 0$  and  $\delta_2 = o_\delta(1)$  is the parameter occurring in (52). (Note that this is possible since  $\alpha$  is a continuity point of  $h$ , so  $m < (1 - \alpha \log 2)^{-1}$ .) Recall the event  $E = E(\varepsilon, \delta, m, \alpha)$  from Lemma 26.

**Lemma 27.** *Fix  $\varepsilon \in (0, 1/2)$  and let  $I$  denote the interval  $I := (k^{1-\beta}, k]$ . For a tuple  $\theta = (\theta_1, \dots, \theta_m)$ , let  $j(\theta)$  denote an index for which  $\|\theta_j\|$  is maximal. Then*

$$(59) \quad \mathbf{E}_{\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}} 1_E |F(\theta)|^2 \ll_{\varepsilon, m} \prod_{\substack{i: 1 \leq i \leq m, \\ i \neq j(\theta)}} (\|k \theta_i\| \vee 1)^{-1+\delta_2}.$$

*Proof.* For each  $1 \leq i \leq m$ , set  $t_i := k \theta_i$  and define the cutoff parameter

$$k_i := \begin{cases} k^\beta, & \|t_i\| \geq k^\beta \\ \|t_i\|, & 1 < \|t_i\| < k^\beta \\ 1, & \|t_i\| \leq 1. \end{cases}$$

Note that  $k_i \geq 1$  and  $k_i \geq \|t_i\|^\beta$ . For each  $1 \leq i \leq m$ , let  $Y_i$  denote the expression

$$Y_i := \sum_{k_i < j \leq k} X_j^{(i)}.$$

By definition of the event  $E$ , when it occurs we have that

$$\sum_{i=1}^m Y_i \geq \alpha(1 - \delta) \sum_{i=1}^m \log k_i - C(\varepsilon).$$

It will be convenient to rewrite this bound in the form

$$(60) \quad 1_E \ll_\varepsilon \prod_{i=1}^m k_i^{-\alpha(1-\delta) \log 2} \prod_{i=1}^m 2^{Y_i}.$$

We define the quantity

$$(61) \quad R = R(\theta, \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}, \varepsilon, \delta, \alpha) := |F(\theta)|^2 \prod_{i=1}^m 2^{Y_i}.$$

To establish the bound (59), we will first show that  $\mathbf{E}_{\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}} R \ll_{\varepsilon, m} 1$ . Once this has been established, it will follow directly from (60) that

$$(62) \quad \mathbf{E} 1_E |F(\theta)|^2 \ll_{\varepsilon, m} \prod_{i=1}^m k_i^{-\alpha(1-\delta) \log 2}.$$

Obtaining (59) from (62) is a simple exercise in lower bounding the maximum of a sequence by its geometric mean. Recalling the definition of  $j(\theta)$  above, we have that

$$k_{j(\theta)} \geq \prod_{\substack{i: 1 \leq i \leq m, \\ i \neq j(\theta)}} k_i^{\frac{1}{m-1}}.$$

Consequently

$$(63) \quad \prod_{i=1}^m k_i^{-\alpha(1-\delta) \log 2} \leq \prod_{\substack{i: 1 \leq i \leq m, \\ i \neq j(\theta)}} k_i^{-\frac{m}{m-1} \alpha(1-\delta) \log 2}.$$

Substituting the lower bound  $k_i \geq (\|k\theta_i\| \vee 1)^\beta$  into (63), we see that (62) implies

$$\mathbf{E} 1_E |F(\boldsymbol{\theta})|^2 \ll_{\varepsilon, m} \prod_{\substack{i: 1 \leq i \leq m, \\ i \neq j}} (\|k\theta_i\| \vee 1)^{-\frac{m}{m-1} \alpha \beta (1-\delta) \log 2},$$

and since  $\frac{m}{m-1} \alpha \beta (1-\delta) \log 2 = 1 + o_\delta(1)$  by definition of  $\beta$ , the desired bound follows.

Finally we justify that  $\mathbf{E}_{\mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}} R \ll_{\varepsilon, m} 1$ . Substituting (56) into (61) yields that

$$R = \prod_{i=1}^m \left[ 2^{Y_i} \prod_{j \in I} \left| \frac{1 + e(j\theta_i)}{2} \right|^{2X_j^{(i)}} \right].$$

Recall that  $Y_i = \sum_{k_i < j \leq k} X_j^{(i)}$  and that  $I = (k^{1-\beta}, k]$ . Thus

$$R = \prod_{i=1}^m \left[ \prod_{k^{1-\beta} < j \leq k_i} \left| \frac{1 + e(j\theta_i)}{2} \right|^{2X_j^{(i)}} \prod_{k_i < j \leq k} \left| \frac{1 + e(j\theta_i)}{\sqrt{2}} \right|^{2X_j^{(i)}} \right].$$

To compute  $\mathbf{E} R$ , we recall that if  $P$  is a Poisson random variable with mean  $\lambda$ , then  $\log \mathbf{E} a^P = e^{\lambda(a-1)}$ . Since the variables  $X_j^{(i)}$  are independent Poisson variables with mean  $\mathbf{E} X_j^{(i)} = \frac{\alpha}{j}$ , it follows after some simplification that

$$(64) \quad \mathbf{E} R = \exp \sum_{i=1}^m \left[ \sum_{k^{1-\beta} < j \leq k_i} \frac{\alpha (\cos(2\pi j\theta_i) - 1)}{2j} + \sum_{k_i < j \leq k} \frac{\alpha \cos(2\pi j\theta_i)}{j} \right].$$

Next we apply the following bound from [EFG15a, Lemma 3.4]:

$$(65) \quad \sum_{j \leq k} \frac{\cos(2\pi j\theta)}{j} = \log \min(k, \|\theta\|^{-1}) + O(1).$$

Substituting into (64) yields that

$$\mathbf{E} R = \exp \alpha \sum_{i=1}^m \left[ \frac{1}{2} \log \frac{k^\beta \vee \|k\theta_i\|}{k_i \vee \|k\theta_i\|} - \frac{1}{2} \log \frac{k^\beta}{k_i} + \log \frac{k_i \vee \|k\theta_i\|}{1 \vee \|k\theta_i\|} + O(1) \right].$$

By definition of  $k_i$ , each summand is  $O(1)$ . Therefore  $\mathbf{E} R \ll_{\varepsilon, m} 1$ , as desired.  $\square$

Finally we integrate the bound (59) with respect to  $\boldsymbol{\theta}$  to obtain a bound on the integral appearing in (58).

**Corollary 28.** *Let  $I = (k^{1-\beta}, k]$  and recall the function  $F(\boldsymbol{\theta}) = F_I(\boldsymbol{\theta})$  from (56). Then*

$$\int_{\mathbb{T}_0^m} \mathbf{E} 1_E |F(\boldsymbol{\theta})|^2 d\boldsymbol{\theta} \ll_{\varepsilon, m} k^{1-m}.$$

*Proof.* After the change of variables  $\mathbf{t} = k\boldsymbol{\theta}$ , the bound reduces to verifying that

$$\int_{k \cdot \mathbb{T}_0^m} \mathbf{E} 1_E |F(\boldsymbol{\theta})|^2 d\mathbf{t} \ll_{\varepsilon, m} 1.$$

Applying Lemma 27, we have

$$(66) \quad \int_{k \cdot \mathbb{T}_0^m} \mathbf{E} 1_E |F(\boldsymbol{\theta})|^2 d\mathbf{t} \ll_{\varepsilon, m} \int_{k \cdot \mathbb{T}_0^m} \prod_{\substack{i: 1 \leq i \leq m, \\ i \neq j(\mathbf{t})}} (\|t_i\| \vee 1)^{-(1+\delta_2)} d\mathbf{t}.$$

By symmetry, we may upper bound the integral (66) by

$$(67) \quad m \int_{k \cdot \mathbb{T}_0^m} \prod_{i=1}^{m-1} (\|t_i\| \vee 1)^{-(1+\delta_2)} dt = m \left( \int_{-k/2}^{k/2} (|t_i| \vee 1)^{-(1+\delta_2)} dt_i \right)^{m-1}.$$

The rightmost integral in (67) is bounded above by

$$m \left( 2 \int_1^\infty t_i^{-(1+\delta_2)} dt_i + 2 \right)^{m-1}.$$

The desired result now follows since the latter integral is finite and independent of  $k$ .  $\square$

Substituting the result of Corollary 28 into (58) lets us show  $|S(I; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)})| \gg k^{m-1}$  with high probability.

**Proposition 29.** *Let  $I = (k^{1-\beta}, k]$ . With probability greater than  $1/2$ ,  $S(I; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}) \subset [-ck, ck]^{m-1}$  for some constant  $c$  and  $|S(I; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)})| \gg k^{m-1}$ .*

*Proof.* By Lemma 25 with  $\varepsilon = 1/3$ , with probability greater than  $2/3$  we have  $\mathcal{L}(I, \mathbf{X}^{(i)}) \subset [0, \frac{3mk}{\alpha}] \subset [0, ck]$  for some constant  $c$  and all  $i$ . It follows that  $S(I; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}) \subset [-ck, ck]^{m-1}$ .

By Lemma 26 with  $\varepsilon = 1/20$ , the event  $E(\varepsilon, \delta, m, \alpha)$  holds with probability greater  $19/20$  and by Corollary 28,

$$\int_{\mathbb{T}_0^m} \mathbf{E} 1_E |F(\boldsymbol{\theta})|^2 d\boldsymbol{\theta} \ll_{\varepsilon, m} k^{1-m}.$$

It follows by Markov's inequality that for some sufficiently large  $L$ ,

$$\begin{aligned} \mathbf{P} \left[ \left\{ \int_{\mathbb{T}_0^m} |F(\boldsymbol{\theta})|^2 d\boldsymbol{\theta} \ll k^{1-m} \right\}^c \right] &\leq \mathbf{P}[E^c] + \mathbf{P} \left[ 1_E \int_{\mathbb{T}_0^m} |F(\boldsymbol{\theta})|^2 d\boldsymbol{\theta} > Lk^{1-m} \right] \\ &\leq \frac{1}{20} + \frac{\mathbf{E} 1_E \int_{\mathbb{T}_0^m} |F(\boldsymbol{\theta})|^2 d\boldsymbol{\theta}}{Lk^{1-m}} \\ &\leq \frac{1}{10}. \end{aligned}$$

It then follows from (58) that with probability at least  $9/10$ ,

$$|S(I; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)})| \geq \left( \int_{\mathbb{T}_0^m} |F(\boldsymbol{\theta})|^2 d\boldsymbol{\theta} \right)^{-1} \gg k^{m-1}.$$

Both events then occur simultaneously with probability at least  $1/2$ , completing our proof.  $\square$

**Proposition 30.** *Let  $D$  be sufficiently large constant and  $I = (k^{1-\beta}, Dk]$ . With probability bounded away from zero there exists an array  $(x_j^{(i)} : 1 \leq i \leq m, j \in I)$  for which*

$$0 \leq x_j^{(i)} \leq X_j^{(i)}$$

for all  $i$  and  $j \in I$ , and

$$\sum_{j \in I} j x_j^{(1)} = \dots = \sum_{j \in I} j x_j^{(m)}.$$



*Proof.* We define the interval  $I' = (k^{1-\beta}, k]$ . By Proposition 29 with probability greater than  $1/2$

$$S(I'; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}) \subset [-ck, ck]^{m-1}$$

and  $|S(I'; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)})| \gg k^{m-1}$ .

Let  $d = 2(5/2)^{1/\alpha}$ . Straightforward calculations tell us that independently with probability greater than  $1/2$  there exists  $j_m \in (2ck, cdk]$  such that  $X_{j_m}^{(m)} > 0$ . Given this  $j_m$ , there are  $\gg k^{m-1}$  collections of constants  $\{j_\ell\}_1^{m-1} \in (ck, (d+1)ck]^{m-1}$  such that

$$(j_m - j_1, \dots, j_m - j_{m-1}) \in S(I'; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)}).$$

Therefore, independently with probability bounded away from zero, there is one such collection  $\{j_\ell\}_1^{m-1}$  such that  $X_{j_\ell}^{(\ell)} > 0$  for all  $\ell$ .

By the definition of  $S(I'; \mathbf{X}^{(1)}, \dots, \mathbf{X}^{(m)})$  we have a set of values  $(n_i \in \mathcal{L}(I', \mathbf{X}^{(i)}))_{i=1}^m$  such that

$$(n_1 - n_m)_1^{m-1} = (j_m - j_\ell)_1^{m-1}.$$

Manipulating the terms coordinate-wise yields

$$j_1 + n_1 = \dots = j_m + n_m.$$

Our claim follows by setting  $D = (d+1)c$ . □

**Corollary 31.**  $\bigcap_{i=1}^m \mathcal{L}(\mathbf{X}^{(i)})$  is almost surely infinite.

*Proof.* We define  $k_1$  to be sufficiently large for Proposition 30 to hold, then inductively define  $k_{i+1} = (Dk_i)^{1/(1-\beta)}$ . The intervals  $I_i = (k_i^{1-\beta}, Dk_i]$  are pairwise disjoint and the set

$$\bigcap_{j=1}^m \mathcal{L}(I_i, \mathbf{X}^{(j)})$$

is non-empty with probability bounded away from zero. Since these events are independent for distinct values of  $i$ , the claim now follows from the second Borel-Cantelli lemma. □

*Proof of Proposition 24.* As we had fixed  $m = h(\alpha)$ , by Corollary 31  $s_\alpha \geq h(\alpha)$  holds for continuity points of  $h$ . For points of discontinuity, we fix  $\alpha' < \alpha$  such that  $h(\alpha') = h(\alpha) = m$ . We couple two sets of independent realizations  $\mathbf{X}^{(1)}(\alpha), \dots, \mathbf{X}^{(m)}(\alpha)$  and  $\mathbf{X}^{(1)}(\alpha'), \dots, \mathbf{X}^{(m)}(\alpha')$  such that  $X^{(i)}(\alpha') \subseteq X^{(i)}(\alpha)$  for all  $i$ . Now  $\bigcap_{i=1}^m \mathcal{L}(\mathbf{X}^{(i)}(\alpha'))$  is almost surely finite by Corollary 31. Our coupling ensures  $\mathcal{L}(\mathbf{X}^{(i)}(\alpha')) \subseteq \mathcal{L}(\mathbf{X}^{(i)}(\alpha))$  for all  $i$ , so  $\bigcap_{i=1}^m \mathcal{L}(\mathbf{X}^{(i)}(\alpha')) \subseteq \bigcap_{i=1}^m \mathcal{L}(\mathbf{X}^{(i)}(\alpha))$ . Thus the second intersection is almost surely infinite, and our claim follows. □

*Proof of Theorem 6.* This now follows immediately from Proposition 23 and Proposition 24. □

## REFERENCES

- [ABT92] Richard Arratia, A. D. Barbour, and Simon Tavaré, *Poisson process approximations for the ewens sampling formula*, Ann. Appl. Probab. **2** (1992), no. 3, 519–535.
- [ABT00] R. Arratia, A. D. Barbour, and S. Tavaré, *Limits of logarithmic combinatorial structures*, Ann. Probab. **28** (2000), no. 4, 1620–1644.
- [ABT16] Richard Arratia, A. D. Barbour, and Simon Tavaré, *Exploiting the feller coupling for the ewens sampling formula*, Statist. Sci. **31** (2016), no. 1, 27–29.
- [Apo76] Tom M. Apostol, *Introduction to analytic number theory*, Undergraduate texts in mathematics, Springer, New York, Berlin, Heidelberg, 1976, Autres tirages : 1984, 1986, 1995, 1998, 2010.

- [AT92] Richard Arratia and Simon Tavaré, *The cycle structure of random permutations*, Ann. Probab. **20** (1992), no. 3, 1567–1591.
- [AT13] ———, *Independent process approximations for random combinatorial structures*, arXiv preprint arXiv:1308.3279 (2013).
- [Bab81] László Babai, *On the order of uniprimitive permutation groups*, Annals of Mathematics **113** (1981), no. 3, 553–568.
- [Bov80] JD Bovey, *The probability that some power of a permutation has small degree*, Bulletin of the London Mathematical Society **12** (1980), no. 1, 47–51.
- [BUV11] Volker Betz, Daniel Ueltschi, and Yvan Velenik, *Random permutations with cycle weights*, Ann. Appl. Probab. **21** (2011), no. 1, 312–331.
- [Cra16a] Harry Crane, *Rejoinder: The ubiquitous ewens sampling formula*, Statist. Sci. **31** (2016), no. 1, 37–39.
- [Cra16b] ———, *The ubiquitous ewens sampling formula*, Statist. Sci. **31** (2016), no. 1, 1–19.
- [Dix92] John D. Dixon, *Random sets which invariably generate the symmetric group*, Discrete Mathematics **105** (1992), no. 1, 25 – 39.
- [DS00] J.H. Davenport and G.C. Smith, *Fast recognition of alternating and symmetric galois groups*, Journal of Pure and Applied Algebra **153** (2000), no. 1, 17 – 25.
- [EFG15a] S. Eberhard, K. Ford, and B. Green, *Invariable generation of the symmetric group*, ArXiv e-prints (2015).
- [EFG15b] Sean Eberhard, Kevin Ford, and Ben Green, *Permutations fixing a  $k$ -set*, International Mathematics Research Notices (2015).
- [ET67] P Erdős and P Turán, *On some problems of a statistical group-theory. ii*, Acta Mathematica Hungarica **18** (1967), no. 1-2, 151–163.
- [EU14] Nicholas M. Ercolani and Daniel Ueltschi, *Cycle structure of random permutations with cycle weights*, Random Structures & Algorithms **44** (2014), no. 1, 109–133.
- [Eul37] Leonhard Euler, *Observationes circa series, infinitas*, Commentarii Academiae Scientiarum Petropolitanae **9** (1737), 160–188.
- [Fel45] William Feller, *The fundamental limit theorems in probability*, Bulletin of the American Mathematical Society **51** (1945), no. 11, 800–832.
- [GM98] Robert Guralnick and Kay Magaard, *On the minimal degree of a primitive permutation group*, Journal of Algebra **207** (1998), no. 1, 127–145.
- [GP16] A. Gladkich and R. Peled, *On the Cycle Structure of Mallows Permutations*, ArXiv e-prints (2016).
- [Gra08] Andrew Granville, *The anatomy of integers and permutations*, preprint.[Ack] (2008).
- [Hei86] Joos Heintz, *On polynomials with symmetric galois group which are easy to compute*, Theoretical Computer Science **47** (1986), 99 – 105.
- [KKRW15] R. Kenyon, D. Kral, C. Radin, and P. Winkler, *Permutations with fixed pattern densities*, ArXiv e-prints (2015).
- [LP93] Tomasz Luczak and László Pyber, *On random generation of the symmetric group*, Combinatorics, Probability and Computing **2** (1993), 505–512.
- [Mal57] C. L. Mallows, *Non-null ranking models. i*, Biometrika **44** (1957), no. 1/2, 114–130.
- [MT84] H. Maier and G. Tenenbaum, *On the set of divisors of an integer*, Inventiones mathematicae **76** (1984), no. 1, 121–128.
- [Muk16] Sumit Mukherjee, *Fixed points and cycle structure of random permutations*, Electron. J. Probab. **21** (2016), 18 pp.
- [Mus78] David R. Musser, *On the efficiency of a polynomial irreducibility test*, J. ACM **25** (1978), no. 2, 271–282.
- [PPR15] Robin Pemantle, Yuval Peres, and Igor Rivin, *Four random permutations conjugated by an adversary generate  $sn$  with high probability*, Random Structures & Algorithms (2015), n/a–n/a.
- [Wae34] B.L. van der Waerden, *Die seltenheit der gleichungen mit affekt*, Mathematische Annalen **109** (1934), 13–16.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WASHINGTON  
*E-mail address:* `gerandy@math.washington.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WASHINGTON  
*E-mail address:* `cff2008@math.washington.edu`

DEPARTMENT OF MATHEMATICS, DUKE UNIVERSITY  
*E-mail address:* `jungem@math.duke.edu`

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WASHINGTON  
*E-mail address:* `avius@math.washington.edu`